TECHNICAL REPORT 1949
October 2006

Using Human Systems Integration and Knowledge Engineering to Define and Design Anti-Terrorism/Force Protection Systems and Solutions

D. Lulue
G. Wilford
D. Gill-Hesselgrave

SSC San Diego

TECHNICAL REPORT 1949
October 2006

Using Human Systems Integration and Knowledge Engineering to Define and Design Anti-Terrorism/Force Protection Systems and Solutions

D. Lulue
G. Wilford
D. Gill-Hesselgrave

SSC San Diego
San Diego, CA 92152-5001

SSC SAN DIEGO
San Diego, California 92152-5001

F. D. Unetic, CAPT, USN	**C. A. Keeney**
Commanding Officer	**Executive Director**

ADMINISTRATIVE INFORMATION

The work described in this report was prepared for the Naval Facilities Engineering Command by User-Center Design Technologies Group (Code 24610) of Space and Naval Warfare Systems Center San Diego (SSC San Diego).

Released by
F. P. Calantropio, Head
User-Centered Design Team

Under authority of
T. Tiernan, Head
Command and Control
Technology and
Experimentation Division

ACKNOWLEDGMENTS

The authors wish to thank Dr. Béla Fehér, John Kammerer, and Frank Calantropio of Code 246210 for their assistance with the field research on which this report is based. Each of these User-Centered Design Technologies Group team members also provided ongoing support during the writing of this publication.

EXECUTIVE SUMMARY

BACKGROUND

In early Fiscal Year (FY) 2006, Naval Facilities Engineering Command (NAVFAC) commissioned a study of current best practices in the Human Systems Integration (HSI) field. The goal for the study was to determine whether supporting up-front analysis and performing early HSI research in the Anti-Terrorism/Force Protection (AT/FP) domain would result in better acquisition decisions.

To conduct a broad-based study, NAVFAC contacted investigators from SPAWAR Systems Center San Diego (SSC San Diego), SPAWAR Systems Center Charleston (SSC Charleston), and Naval Surface Weapons Center Dahlgren Division (NSWC-DD). Of the three organizations invited to contribute to the study, only SSC San Diego and SSC Charleston supplied content to this final report. NSWC-DD dropped out of the project and did not provide any content to this report.

The two investigational teams decided to leverage the unique expertise of their organizations. SSC San Diego looked to its in-house human factors engineering and user-centered design experts to research the work being done by watchstanders in Regional Operation Centers (ROCs). Based on that research, the San Diego team developed a prototype command and control (C2) system that supports the actual processes and information requirements of ROC watchstanders. The SSC Charleston team used its human factors engineering and HSI experts to perform a pre-design analysis to determine the functional user requirements (FURs) necessary to design and upgrade an AT/FP Operations Center.

Throughout the study, the two teams used HSI practices to identify opportunities to make improvements in their targeted areas of research. Performed correctly and early in an acquisition process, HSI practices can reveal ways to reduce staffing levels, improve training curricula and reduce costs, improve environmental and health/safety conditions, and so on. When Knowledge Engineering (KE) and business process modeling (BPM) results are factored into the analysis—which both teams did—improvements can also be made to the investigated organizations' processes, which can result in process re-engineering recommendations to those organizations' decision-makers.

Both team studies began by investigating the physical, virtual, and work process spaces of their target organizations. Through their field work, the investigators aligned the evidence they collected with the following HSI characteristics:

- Manpower
- Personnel
- Training
- Safety and Health
- Habitability
- Personnel Survivability

The teams also used the Knowledge Engineering/Human Systems Integration (KE/HSI) model to evaluate the relevance of their proposed system or solution to the targeted AT/FP domain they were investigating.

THE IMPORTANCE OF HSI

Many program managers wonder why they should pay to incorporate HSI activities into their programs. Justifying HSI can be a challenge. There are precious few metrics to support a manager's decision to include HSI in their programs, but there are ample anecdotal examples of the cost for not including a well-reasoned and appropriately scaled HSI approach early in a program.

Three articles recently published in the *Washington Post*, the *Associated Press*, and the *Chicago Tribune* show how ignoring a few important HSI practices can lead to costly, ineffective systems. The following HSI practices could have avoided these undesirable results:

- Collect data about what the customer wants and users require
- Understand the importance of key business processes
- Consider environmental factors that can delay deadlines and increase costs

According to the *Washington Post* (18 August 2006), the FBI had contracted out the development of a networked system for tracking criminal cases. After spending $170 million, the FBI still had an archaic computer system and had to restart development. The article stated that "the collapse of the attempt to remake the FBI's filing system stemmed from failures of almost every kind, including poor conception and muddled execution of the steps needed to make the system work."

If an HSI process had been in place on this project, data could have been collected about what the customer wanted and what the users required. By using an HSI process, the program manager for this endeavor would have had performance metrics that could have been used to measure, early and often, the developer's progress to the goal of a useful, usable system within the time and dollar constraints of the program.

To read the complete article, see the following *Washington Post* Web site:

http://www.washingtonpost.com/wp-dyn/content/article/2006/08/17/AR2006081701485.html.

An Associated Press article published in the *Flagstaff Arizona Sun* reported that the Internal Revenue Service lost $200 to $300 million in 2006 because an inoperable computer program designed to screen tax returns for fraudulent claims had caught only 34 percent of the fraudulent claims that had been caught by that time in 2005. The inoperable computer program cost the Government $21 million.

If the developer had more fully understood the customer's key business processes and had accurately reflected them in the solution that was delivered, much if not all of the software development problems cited could have been mitigated.

To read the full article, see the Flagstaff Arizona Sun Web site:

http://www.azdailysun.com/articles/2006/07/15/news/20060715_news_37.prt

According to the *Chicago Tribune* (27 August 2006), many experts had questioned whether the intricate Sea-Based X-band (SBX) radar on a vessel traveling from the Gulf of Mexico to a port in Alaska could survive the tumultuous waters the SBX would encounter on the trip. The massive SBX was damaged during its voyage and docked in Hawaii for more than 8 months.

Common sense about the system's physical operating environment seems to have been missing from the onset of this program. Environmental considerations are a major HSI characteristic, which if known early, can lead developers to solutions that meet the requirements of the system's intended milieu.

To read the complete article, see the *Chicago Tribune* Web site:

http://www.chicagotribune.com/news/nationworld/chi-0608270359aug27,0,3725134.story?coll=chi-newsnationworld-hed

RECOMMENDATIONS

As a result of their independent studies, the SSC San Diego and SSC Charleston teams firmly found that when HSI principles are included during up-front analysis and when HSI-based analysis is performed throughout the entire acquisition process, more successful programs can be deployed into the AT/FP domain.

As a set of principles, HSI can inform every phase of the research, development, testing and evaluation cycle to help ensure that the best possible acquisition decisions are made. Based on their analyses, the two teams offer the following recommendations.

SSC San Diego

From their HSI investigations at several Regional Operation Centers (ROCs), a Regional Dispatch Center (RDC), and a Sector Command Center, SSC San Diego recommends the following training improvements:

- An important goal is to move away from today's dislocated training methodology to one that seamlessly trains students to efficiently perform operational workflows within the organization's mission context while using the organization's embedded systems, which were originally designed to support realistic tasks and workflows rather than atomic functions.
- Systems installed in Civil-Military Operations Centers (CMOCs), ROCs, and RDCs should explicitly support operational processes. The human–computer interfaces (HCIs) should provide on-the-glass task visualization of operational processes, and the Web services that make up the application and business logic should be direct models of an organization's operational processes. When this goal is achieved, an end-to-end, hands-on training curricula can be devised that prepares students for easy integration into the organization's mission.
- By creating training curricula and training models that teach application functions in the context of the roles and responsibilities of the job, operators will become more effective system users and more successful staff members.

Based on field visits and interviews, knowledge- and process-model development, and personnel and mission analyses, SSC San Diego recommends the following KE improvements:

- Performing a complete and formal HSI study focused on RDC training, manning, and HFE across all of the Navy regions is clearly needed.
- Performing a follow-on KE effort scoped to the entire AT/FP domain would lead to discovery of real-world AT/FP processes and tasks. The complete KE model set would enable NAVFAC to devise realistic concept of operations (CONOPS) and standard operating procedures (SOPs) for all ROCs and RDCs, promoting standardization and helping to reduce the overall training load.
- Standardization of training and internal processes needs to be increased across the regions. A trained person should be able to function in any region's RDC or ROC and be familiar with its processes and systems.

- Focusing on those activities that lend themselves to direct and concrete actions is always tempting. In the AT/FP domain, constructing a physical plant, installing duplicative systems, and focusing on electromagnetic and dispatch tasks appear to receive the most emphasis. Efforts to understand, model, and solve the class of problems associated with AT/FP appear to be de-emphasized. While this class of problems is particularly difficult to attack, they represent the first line of defense. If they are solved, then terrorist-generated emergencies will be better managed and less force reconstitution burdens will occur.

- Focusing attention on the concept of virtual ROCs as opposed to physical ROCs would be valuable. A virtual ROC could be stood up through network reconfiguration and discoverable Web service deployment. If the standardization and cross-training recommendations already noted here are implemented, then the virtual ROC's personnel will be prepared to execute at high-efficiency levels 24/7 from any location. Specifically, they would all be able to perform a wide variety of tasks across anti-terrorism, force protection, emergency management, and dispatch within a standardized set of processes without regard for their geographic relationship to one another or to the event(s).

- Requiring compliance on the part of system providers with Department of Defense (DoD) Global Information Grid (GIG) and network-centric requirements is of paramount importance. When pre-existing, non-Navy Community Engagement Strategy-compliant systems are installed, training and manning are adversely impacted.

SSC Charleston

Based on the findings and analysis from their FUR methodology, SSC Charleston recommends the following Command Center Design improvements:

- Require the use of the FUR methodology for all AT/FP Operations Center programs*
- Explore the use of the FUR methodology in other AT/FP technology areas
- Require compliance on the part of system providers with DoD GIG and network-centric requirements

CONCLUSION

Clearly, ignoring the application of HSI principles can have serious negative effects on program results. When programs fail, a feeding frenzy among the media often occurs. But even more important than saving face in front of the media or avoiding public scrutiny of failures, programs should strive to avoid the pitfalls that ignoring HSI principles cause by ensuring the development and delivery of systems and solutions that are useful to and usable by the intended users.

On 13 September 2006, Frank W. Deffer, Assistant Inspector General for Information Technology for the U.S. Department of Homeland Security, presented a report to the Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment.

---

* Operational Centers include Emergency Operations Centers (EOCs) and Mobile Command Posts (MCPs).

In his statement, Mr. Deffer reported that the following program decisions led to the failure of a major Department of Homeland Security initiative, the Homeland Security Information Network (HSIN):

- Rushed schedule
- Lack of clear definition regarding the relationship of the program to existing systems
- Developing and deploying the program in an ad hoc manner
- Not providing adequate guidance to the intended users
- Not establishing performance metrics

Mr. Deffer's remarks indicate that had HSI principles been applied early and often throughout HSIN's lifecycle, the effectiveness of the program's systems and solutions, and their adoption by the intended user community would have resulted in a successful deployment of a useful and usable set of systems and solutions to the intended user community and to related stakeholder communities.

According to Mr. Deffer, if the correct up-front investigations and appropriate "follow-along" work had been performed, the following program benefits would have been realized and the failures cited in the Office of Inspector General's report[†] would not have occurred or would have been substantially mitigated. Among the benefits that Mr. Deffer notes in his remarks to the Subcommittee were the following:

- Clarifying the program's mission and vision to the intended users, especially its relation to other systems and solutions, and their integration into the established workflow and mission of the intended users
- Defining the information needs and workflow models of the intended users so the program's systems and solutions support the intended users' rather than the users' supporting the systems
- Providing detailed support specific to the needs of the intended users in the form of SOPs procedures, user manuals, and training based on the business processes needed by the intended users to achieve their assigned missions (which can only be established by understanding the information needs and workflow models of the intended users).
- Ensuring representation and participation among various stakeholder communities to deterring business and system requirements
- Identifying baseline and performance metrics and measuring effectiveness using the performance data collected throughout the lifecycle of the program's systems and solutions

Clearly, attending to the processes encompassed by HSI principles can substantially improve the probability that a program's systems and solutions will fully support the intended mission, users, and stakeholders. Ignoring or overlooking one or more of the elements of HSI principles puts programs at risk of failure from the outset and can result in unacceptable costs.

[†] Department of Homeland Security Inspector General. 2006 (June). "Homeland Security Information Network Could Support Information Sharing More Effectively." OIG-06-38. Washington, DC. See Appendix A.

CONTENTS

Figures

Tables

INTRODUCTION

This report provides details on two studies that were conducted independently in an attempt to answer the question: "Will doing good front-end analysis and conducting early Human Systems Integration (HSI) research improve the quality of the systems and products that result from Anti-Terrorism/Force Protection (AT/FP) acquisition decisions?"

APPROACH

The study contributors, SPAWAR Systems Center San Diego (SSC San Diego) and SPAWAR Systems Center Charleston (SSC Charleston), used a novel approach to answer this investigational question. Each Center performed a work domain/HSI analysis on a work area that was relevant to the AT/FP domain and in which the Center had expertise. Specifically, SSC San Diego focused on Command, Control, Communications, Computers and Intelligence while SSC Charleston investigated Command Center Design.[1]

This report provides study analyses, findings, and improvement recommendations based on work domain data collected by SSC San Diego and SSC Charleston. "Worked examples" of how to best use HSI, Knowledge Engineering (KE), Business Process Modeling (BPM), and User-Centered Design (UCD) elements to investigate, model, and re-engineer AT/FP processes are included in this report. The authors' hypothesis throughout their investigations was that by following these processes and applying the principles of HSI, KE, BPM, and UCD, key decision-makers and customers of the acquisition process can make more informed decisions.

Because funding and schedule limited the study's scope, the investigators scaled their efforts to a representative subset of the AT/FP capability areas. If the findings in this report are deemed meaningful and useful, then a more robust follow-on effort should be planned in order to develop a complete process re-engineering roadmap across the AT/FP domain. Through a larger effort, NAVFAC could use the optimized process models to guide and direct its subordinate commands in making the best use of their physical, computational, and personnel resources.

METHOD

The investigators used a number of methodologies and research techniques to explore and analyze the processes, issues, needs, and requirements of their target capability areas. Some methods used included the following:

- HSI
- KE
- Process Modeling
- UCD

HSI

Fitting the workplace to the worker is fundamental to developing systems and solutions that maximize productivity and operational effectiveness while protecting operators and maintainers from accidents and injury.

---

[1] Early in the design of this study NSWC-DD had planned to examine processes associated with acquiring AT/FP technologies. NSWC-DD dropped out of the project and did not contribute any content to this report.

By using the HSI characteristics shown in Figure 1 as touchstones throughout the research and analysis phase, Human Factors Engineers (HFEs) make their decisions based on rational evidence rather than arbitrary preferences and assumptions.

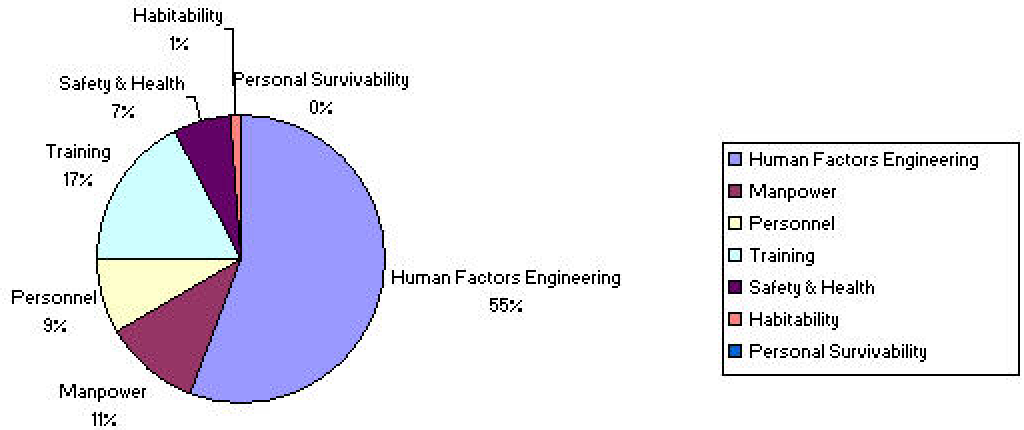

Figure 1. ROC HSI observations distributed across the seven HSI characteristics.

Within these characteristics are constraints, criteria, end-products, and assessments. Table 1 lists the elements within each characteristic. Depending on the scope, purpose, and intended audience for any given project, human factors professionals and their project sponsors and stakeholders need to determine which of these seven characteristics apply to their project and determine which elements of each characteristic are relevant to their analysis.

One method is to embark on the research phase of the project and actively seek out workplace examples that align with each element of each characteristic. Another method, and the one used in this study, is to perform the workplace investigation (observations and interviews) and align the resultant findings with the elements in each characteristic that are relevant to the project.

KE

Dr. Dickson Lukose of the Department of Mathematics, Statistics, and Computer Science, University of New England, Armidale, provides a useful definition of KE engineering:

> "Knowledge Engineering is the technique applied by knowledge engineers to build intelligent systems: Expert Systems, Knowledge Based Systems, Knowledge based Decision Support Systems, Expert Database Systems, etc. There are two main views to knowledge engineering. … The [second] view is known as the 'Modeling View'. In this view, the knowledge engineer attempts to model the knowledge and problem solving techniques of the domain expert into the artificial intelligent system."[2]

[2] http://pages.cpsc.ucalgary.ca/~kremer/courses/CG/CGlecture_notes.html

Table 1. Seven major HSI elements with their respective sub-elements.

Human Factors Engineering	Manpower	Personnel	Training	Safety and Health	Habitability	Personnel Survivability
Physical and Mental Capabilities Limitations	Wartime Requirements	Personnel Classification and Selection	Training Concepts & Strategies	System Safety/Health Plan	Quality of Life	Anti-fratricide
Anthropo-metrics and Biomedical Criteria	Deployment Consideration	Demographics	Task Analysis Methods	Human Error Analyses	Quality of Work	Personnel Protection
Man-Machine Interface	Force Structure	Accession and Attrition Rates	Media / Equipment	System Reliability Analyses	Environment Limits and Controls	Performance Effects of Ensembles
Mission, Function, and Human Requirements Analyses	Operating Strength	Retention Rates	Simulation	Lessons Learned	Personnel Services	Damage Control
Skill, Know-ledge, and Abilities	Manning Concepts	Career Progression	Operational Tempo	Environmental Considerations		Damage Control
Performance Assessments	Officer and Enlisted Workload	Training Flow	Training System Evaluation	Protective Equipment		
			Training Develop-ment Plan			

One KE practice is to develop an ontology.[3] An ontology is a formal concept specification or knowledge representation. Ontologies enable domain experts to use a compact notation to catalogue and annotate their specialized domain knowledge. A knowledge representation is extremely valuable for knowledge sharing, reuse, and subsequent process modeling. A process model complements the knowledge representation, and is constructed with data gathered during field studies[4] and interviews with users, watchstanders, and subject-matter experts.

Process Modeling

Several established methodologies for modeling workflows and business processes exist. Each methodology has associated notations and engines. Business Process Modeling, for example, is the discipline of defining and documenting business practices, processes, information flows, data stores and systems. Graphical process representations can be captured in one of several notations, including the Business Process Modeling Notation (BPMN) or the Business Process Modeling Language (BPML). Several companies provide business process engines that can execute one or more languages.

[3] http://www-ksl.stanford.edu/kst/what-is-an-ontology.html
[4] "Ethnographic Study" is synonymous with "field study" in Knowledge Engineering.
Reference: http://www.otal.umd.edu/hci-rm/ethno.html

Workflow analysis is closely related in that it involves observing and modeling processes to enhance their efficiency and effectiveness. Several workflow modeling notations, languages, and language processing engines are available.

Regardless of the specific notation or language, process modeling involves representing the expert's understanding of the domain in a standardized abstract notation, and then modeling the domain's existing processes. An analyst then reviews the notation and the modeling for duplication, choke points, and re-factoring opportunities. The result is a re-engineered, "formative"[5] knowledge representation and process (or work) flow.

UCD

UCD borrows heavily from agile software development[6] and is composed of two phases:

1. The work domain research phase, and
2. The analysis phase in which the knowledge representation is built.

The first phase typically lasts 4 to 6 weeks. This phase is followed by an open-ended design/develop/test phase made up of a series of 9- to 12-week cycles or spirals.

Correctly implemented, UCD achieves results through better system design. A multi-disciplinary methodology, it involves engineers, computer scientists, designers, HFEs, psychologists, subject-matter experts, and system users. UCD and cyclic-iterative development go hand-in-hand.

The UCD analysis phase determines user visualization, interaction, and content (data) requirements. It also provides process insights that enable human factors professionals to identify process and system improvements. A primary goal is to discover a small and manageable set of "focal" tasks. If these tasks are supported through a set of proposed tools, the UCD investment in will pay off as users' operational efficiency continues to increase.

The UCD up-front analysis phase produces the following artifacts:

- Domain Model (similar to DODAF OV-1)
- Role Model (work roles assumed by users)
- Task Model (user tasks)
- Role/Task Matrix (a task/role histogram)
- Increment Release Map (the UCD version of a software development schedule)

---

[5] Three levels of process description exist: "Normative" (what the organization's official policies say the process should be), "Descriptive" (how the process is executed in actual practice in the field), and "Formative" (how the process could be re-engineered to be more effective or efficient).

[6] The agile software development process is defined in the Wikipedia as "...a conceptual framework for undertaking software engineering projects. There are a number of agile software development methodologies, such as those espoused by the Agile Alliance, a non-profit organization. Most agile methods attempt to minimize risk by developing software in short timeframes, called iterations, which typically last one to four weeks."

SSC SAN DIEGO FINDINGS, ANALYSIS, AND RECOMMENDATIONS

Human factors engineering and UCD experts from SSC San Diego researched the work being done by watchstanders in Regional Dispatch Centers (RDCs), the U.S. Coast Guard San Diego Sector Command Center-Joint (SCC-J), and in three Regional Operation Centers (ROCs): Command Navy Region Hawaii, Command Navy Region Southwest, and Command Navy Region Mid-Atlantic.

HUMAN SYSTEMS INTEGRATION

ROC Training Observations

Regional Operational Centers are fully staffed during regional exercises and real-world emergency events. Unlike operators and watchstanders in Dispatch Centers and Sector Command Centers, ROC staffs do not receive day-to-day training and operational experience. Fleet Command Centers, on the other hand, are staffed 24/7 and led by a senior officer with operational experience. Transitioning Fleet Command Center staffs to ROC staffs during AT/FP exercises and emergencies is therefore a rational fit. Training of personnel who do not perform specific AT/FP tasks during their regular duties is therefore critically important. Such training includes the following:

- Monthly training on operations-related topics and lessons learned
- Specialized training in emergency management, AT/FP policy, and environmental issues
- Exercises such as RogueX, Bayshield, Hurrex, Solid Curtain, port operations, and U.S. Coast Guard drills

RDC Training Observations

Regional Dispatch Center site visits were limited to two RDCs, with one interview opportunity during each visit. The HSI observations were therefore not representative of all the functioning RDCs across all regions. The methodology and preliminary results were instructive, however, and add to the case for follow-on and more formal ethnographic studies across all regions. Within the limited study of 92 total HSI observations, 16 observations (17%) were related specifically to training (Figure 1). Appendix B includes a more detailed listing of these observations, which range from issues related to Federal Police personnel working AT/FP tasks with no AT/FP training to a lack of training on embedded systems.

When the workforce perceives that training is an issue, overall performance suffers. SSC San Diego's analysis suggests that less than optimal performance across four HFE attributes can be attributed to the following ineffective or non-existent training models:

- Skill, Knowledge, and Abilities
- Mission, Function, and Human Requirements Analysis
- Physical and Mental Capabilities and Limitations
- Performance Assessments

Within the 16 observations related to training, five observations pointed directly to the lack of training concepts and strategies and seven observations indicated a deficiency in adequate training development plans. The remaining observations are currently unassigned because finding their root causes requires further investigation.

The Current Training Paradigm

Center training typically develops through several separate steps. First, training needs must be determined. A command might recognize that a new system is being implemented and request system training, or training might be generated as part of a system's original implementation plan. Once the need for training is determined, a third party outside of the operators' organization, and usually outside of the system's designers/developers, is tasked with developing a curriculum to teach the system. This trainer proceeds to develop a curriculum that focuses almost solely on teaching the application's "buttonology." Occasionally, interim training on the application's underlying conceptual construct is provided to the students, but usually this occurs only as a stopgap measure when training is required to begin by a certain date and the final application and/or the curriculum for training on that application is not ready for use by the students.

Buttonology training may or may not be presented in the actual operational workflow context in which the student will work. Preliminary investigations suggest that buttonology-style training is usually delivered in isolation from the conceptual and operational rationales that adult learning theory tells us are essential to success in adult learners. Additionally, this function-based training (that is, training on navigating between windows, how to connect to data sources, and tips on dealing with the idiosyncrasies of different stand-alone applications) does not tend to support a command's need for operators to understand how their interaction with a system affects and supports the success of the command's goals and mission.

The current training model teaches students how to use an application's functions without aligning and correlating that information to the organization's actual workflow steps and the business rationale behind those steps. With such a serious gap between the buttonology with which students are presented and the actual organizational tasks and workflows, students must rely on other sources—usually trial and error and support from more senior staff members—to become fully successful at their assignments.

Once students are integrated into a Center's staff and undergo on-the-job training, they receive instruction in their day-to-day responsibilities and duties. Once again, this instruction is usually isolated from the button-pushing instruction the students have received on the systems they will use to perform their day-to-day duties and responsibilities.

Train the Job by Training the System

To be successful, the students must learn about the organization's overall mission and its goals and constraints. When students receive function-based training through on-the-job training or on an as-needed basis, opportunities for enhanced success and more rapid awareness of the relationships between a Center's systems and job functions are lost.

In short, the typical application training program suffers from the way that stand-alone and proprietary systems are developed and delivered to Department of Defense commands. System design usually begins well with an overall workflow and task analysis. However, the work items and tasks are then broken down into individual steps that are captured in each application as independent actions. These atomic activity units are what students are trained to perform by organizational staff, who must reconstruct the original work items, tasks, and workflows during on-the-job training.

Recommendations

An important goal is to move away from today's dislocated training methodology to one that seamlessly trains students to efficiently perform operational workflows within the organization's mission context while using the organization's embedded systems, which were originally designed not on atomic functions, but on realistic tasks and workflows.

Systems installed in Civil–Military Operations Centers (CMOCs), ROCs, and RDCs should explicitly support operational processes. The HCIs should provide on-the-glass task visualization of operational processes, and the Web services that make up the application and business logic should be direct models of an organization's operational processes. When this goal is achieved, an end-to-end, hands-on training curricula can be devised that prepares students for easy integration into the organization's mission. By creating training curricula and training models that teach the application functions in the context of the roles and responsibilities of the job, operators will become more effective system users and more successful staff members.

KNOWLEDGE ENGINEERING

Field visits were conducted at the following locations:

- Third Fleet Commander Maritime Operations Center
- Navy Region Southwest ROC
- Navy Region Hawaii ROC
- Sector Command Center-Joint

The number of visits and personnel interviews was limited to some extent by funding and schedule constraints. However, HFEs did construct several knowledge and process models.

Knowledge Representations/Process Models

The human factors engineering team modeled the surveillance systems and dispatch systems of one RDC. The team also modeled the RDC's personnel, mission, and basic dispatch process. They derived their models from two site visits (described in site visit reports in Appendix C).

Figure 1 depicts a specific unnamed RDC's surveillance systems. The notation is a Unified Modeling Language (UML) static structure. An open-arrow line shows generalization from a super- class to a subclass. This notation is often used in software development, but can also be used to represent real-world concepts and objects. An industry-standard modeling notation, it is compact and supports many drawing applications. Figure 2 defines the notation's symbols.

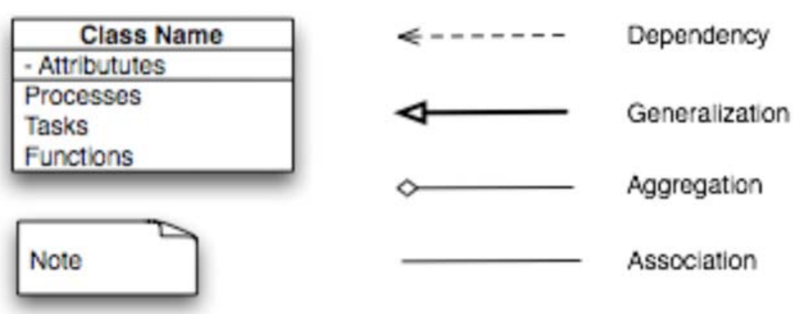

Figure 2. UML static structure notation.

The unnamed surveillance system model in Figure 3 shows a noteworthy lack of duplication, which is in contrast to other RDCs that have multiple proprietary video surveillance systems. Furthermore, in keeping with the current practice of installing multiple proprietary systems, each system has its own specialized user interface and offers feature sets that often overlap with its competitor's feature sets.

Note also that two instances of the active Surveillance class exist: Alarms and Cameras. Data were insufficient to further subclass the Alarm class, but a subsequent site visit would yield the specific types of alarms that feed into the RDC, and which the watchstanders must service. Once the various instances of Camera class are captured, it becomes possible to identify their roles in the RDC's process diagrams, which in turn makes it possible to look for redundancy and opportunities for parallel operations.

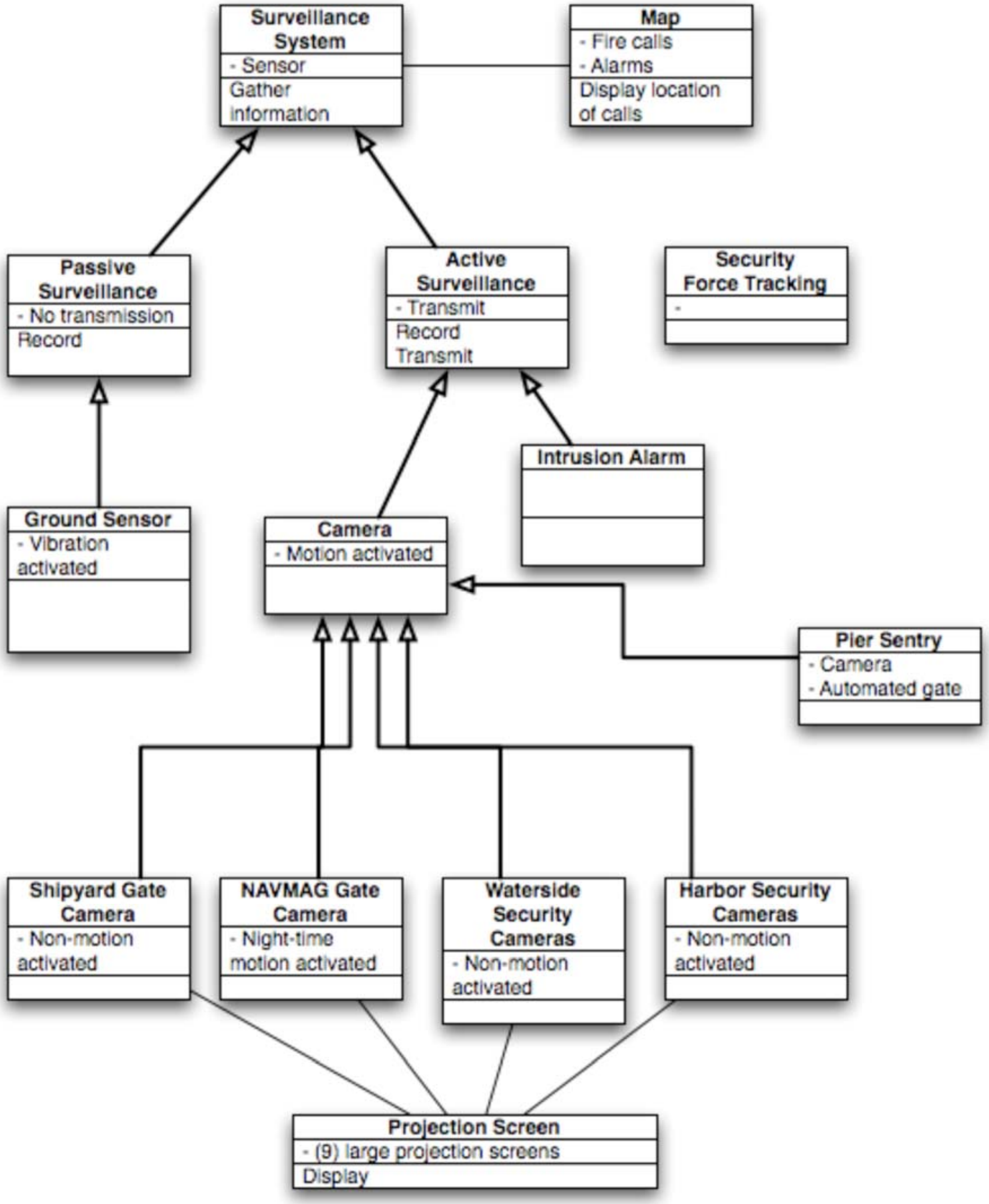

Figure 3. Region “X” RDC surveillance systems model using UML static structure notation.

Figure 4 is a UML static structure model of the same RDC's dispatch systems. Clearly, a follow-up site visit is necessary to "fill out" this model and detail its internal class relationships and external relationships with the surveillance systems. The model that the field report is based on did not provide enough detail to develop all the relationships—hence the requirement for multiple site visits while performing an ethnographic study.

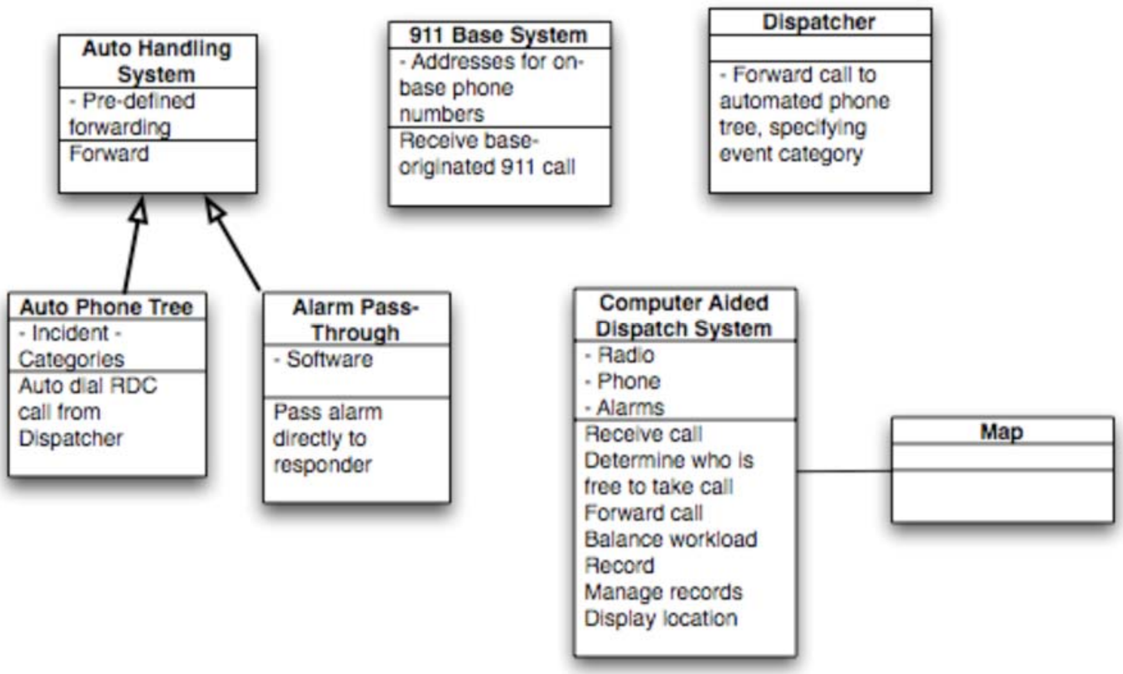

Figure 4. Region "X" RDC dispatch systems.

Figure 5 is a combined model of the Region “X” mission area and personnel.

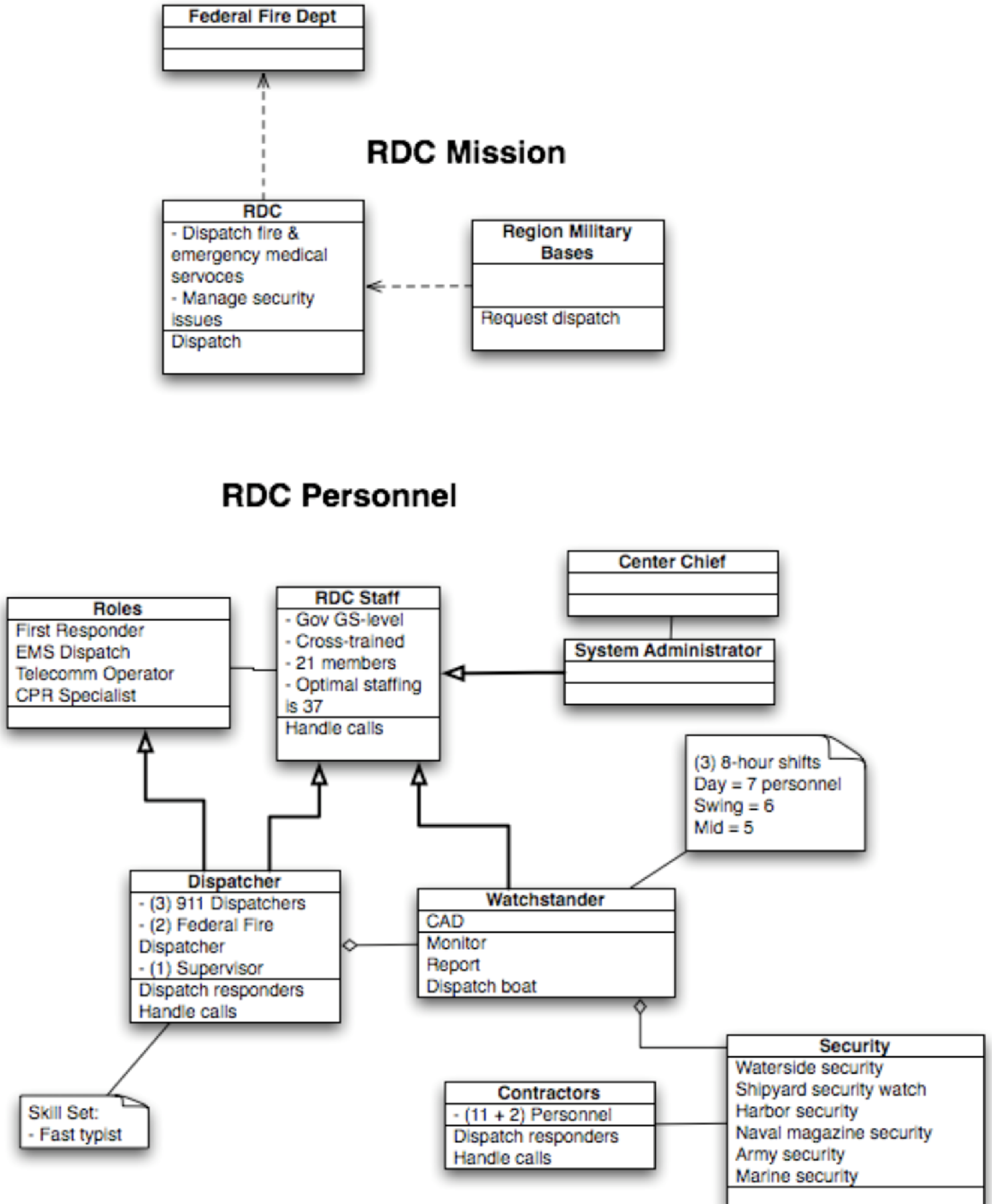

Figure 5. Region “X” mission and personnel.

This region’s RDC is Federal Fire Department-based, while other regional RDCs are Federal Police Department-based. As such, this region emphasizes emergency response and dispatch, as the model makes clear. The AT/FP missions are of secondary importance at this node. Other items of note include the aggregation of security billets and their relationship to the Watchstander class and the Dispatcher class. The RDC's training SOPs include extensive personnel cross-training, as captured in the model. This model provides for skill-set redundancy among staff members and is a good model for all RDCs.

Figure 6 is the Region "X" dispatch process diagram. Each box represents a complex process and could subsequently be broken down into its constituent processes, tasks, and steps.

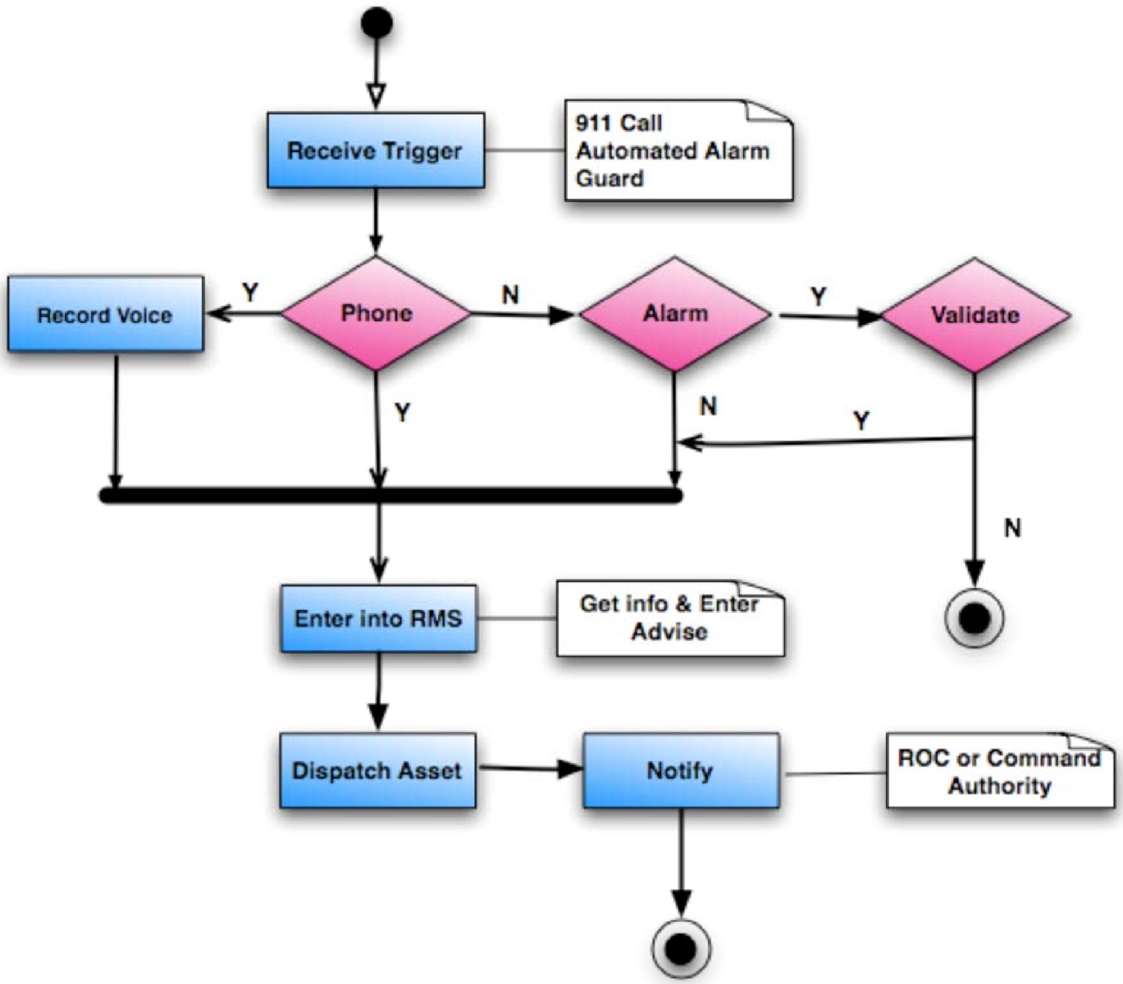

Figure 6. Region "X" high-level dispatch process diagram.

Elaborating on this diagram would be very valuable not only for RDC "X", but for all of the other region's RDCs. Similar diagrams undoubtedly exist, but recall the three kinds of descriptions discussed earlier (see Footnote 5): Normative, Descriptive, and Formative. Any currently existing process diagrams are undoubtedly based on theoretical, official policy, and are therefore *normative* depictions of how things are *supposed to work*. The significance of the simple process diagram in Figure 6 is that it is the *descriptive* form based on a field ethnographic study of actual practice dispatch processes in one RDC. The power of extending this modeling effort across all regions is that their processes could then be compared against a set of AT/FP process standards. Any deficiencies could then be corrected through process re-engineering. Furthermore, any discovered processes that appear to work better in practice than mandated processes could be deployed to all of the other RDCs.

Figure 7 is a Rogue Ship exercise (RogueX) process flow diagram. Its value lies in depicting a real-world, AT series of events. The exercise involves multi-jurisdictional and multi-region coordination and collaboration. It also involves Navy vessels as active participants in an AT operation. AT/FP planners and system developers will benefit greatly from a rich set of subprocesses and tasks that may be discovered in a subsequent investigation.

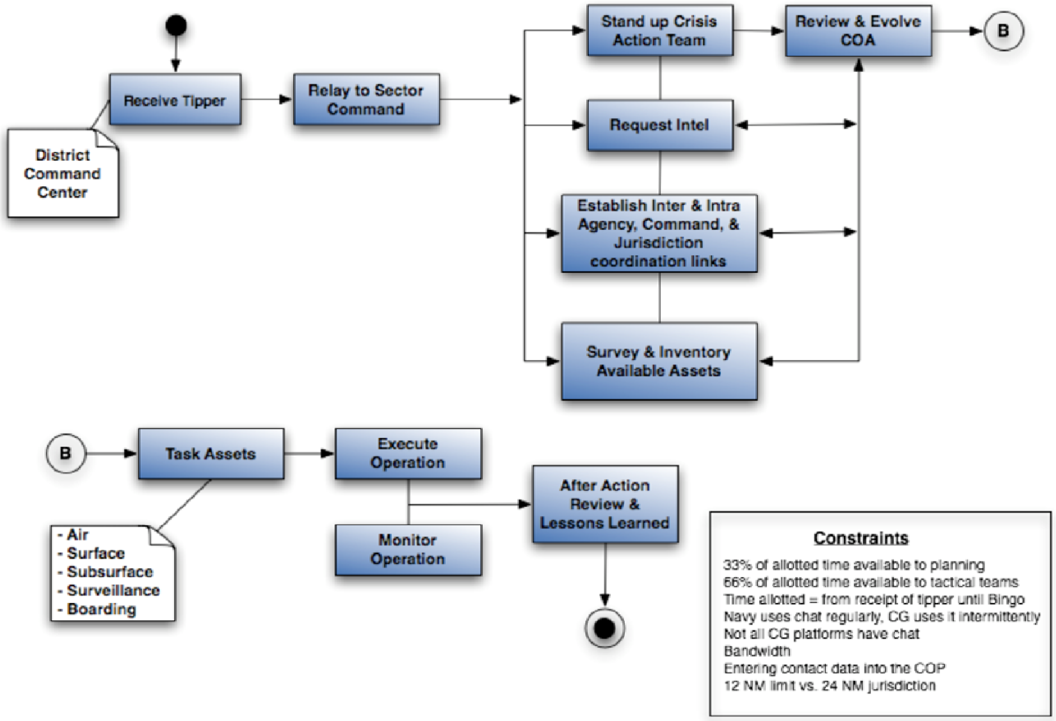

Figure 7. Vessel of interest exercise process flow diagram.

Figure 8 depicts a typical intelligence gathering, research, analysis, assessment, and dissemination process that represents the breakout of one of the process boxes (Request Intel) from Figure 7, the vessel of interest exercise process flow diagram.

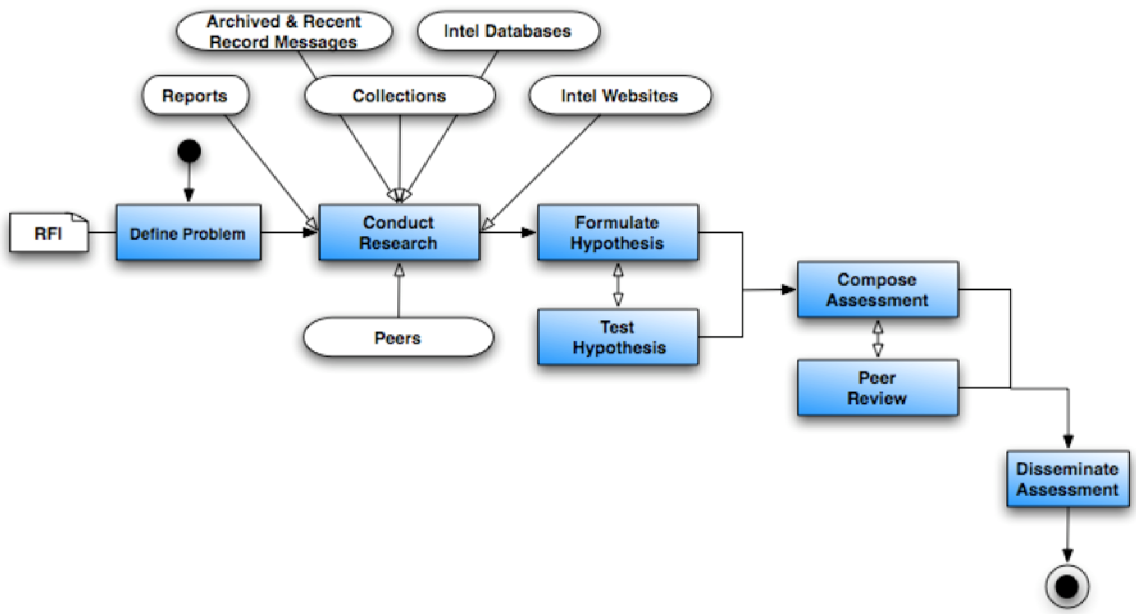

Figure 8. “Request Intel” subprocess from vessel of interest exercise process flow diagram.

Recommendations

Clearly, a complete and formal HSI study focused on RDC training, manning, and human factors engineering across all of the regions is needed.

Performing a follow-on KE effort scoped to the entire AT/FP domain would lead to discovery of real-world AT/FP processes and tasks. The complete KE model set would enable NAVFAC to devise realistic CONOPS and SOPs for all ROCs and RDCs, promoting standardization and helping to reduce the overall training load.

Standardization of training and internal processes needs to be increased across regions. A trained person should be able to function in any region’s RDC or ROC and be familiar with its processes and systems.

Focusing on those activities that lend themselves to direct and concrete actions is always tempting. In the AT/FP domain, constructing a physical plant, installing duplicative systems, and focusing on electromagnetic and dispatch tasks appear to receive the most emphasis. Efforts to understand, model, and solve the class of problems associated with AT/FP appear to be de-emphasized. While this class of problems is particularly difficult to attack, they represent the first line of defense. If they are solved, then there will be few or no terrorist-generated emergencies to manage and no force reconstitution burdens.

Focusing attention on the concept of virtual ROCs as opposed to physical ROCs would be valuable. A virtual ROC could be stood up through network reconfiguration and discoverable Web-service deployment. If the standardization and cross-training goals are met, then the virtual

ROC's personnel are prepared to execute at high-efficiency levels 24/7. They would all be able to perform a wide variety of tasks across AT, FP, emergency management, and dispatch within a standardized set of processes.

Requiring compliance on the part of system providers with Department of Defense Global Information Grid and network-centric requirements is of paramount importance. When pre-existing, non-Navy Community Engagement Strategy-compliant systems are installed, training and manning are adversely impacted.

USER-CENTERED DESIGN

In addition to the Quarter 1 (Q1), Fiscal Year (FY) 2006 HSI work, SSC San Diego conducted extensive UCD investigations into actual-practice AT/FP processes and tasks. The work directly supports the Information Management Pilot Project (IMPP) and is ongoing as of this writing. A separate report on the Q1 findings and models is in preparation. Two of the Q1 UCD artifacts, the Task Model and the raw Domain Models, are included in Appendix C.

Work Domain Analysis and Modeling

Work Domain Analysis is the process of learning as much as possible about a person or work group's workspace within time and funding constraints. A workspace is the physical and virtual environment that contains all of a person's or workgroup's products. A workspace is also the structural constraints—both physical and virtual—that frame the production or activity area. A workspace also shapes enterprise- and employee-developed processes, and affects tasks performed by individuals and groups. A work domain analysis is characterized by three elements:

1. Start-of-project, "up-front" research and analysis
2. Modeling the work in physical, computational, and virtual environments
3. Identifying the users, their roles, and tasks

Once the domain analysis is complete, the design and development team creates a model of the findings. Work domain modeling illustrates the most critical facts about the workspace. The models can be simple or they can be complex. The following subsections describe the UCD elements as applied to this study.

The domain model describes the problem the design is attempting to solve and the environment in which the solution must be implemented. It contains a general description of users, customers, hardware, and spaces. Users include *direct* users and *indirect* users. *Direct users* are the hands-on users of the solution. *Indirect users* are colleagues and collaborators of the direct users.

User Task Analysis and Modeling

Task analysis may be the lynchpin activity of the entire HSI process because it defines the tasks that users perform to complete their roles. User task analysis describes what tasks users do, but does not expose how they do their tasks (it is a technology-independent description of behaviors). During this phase, although only the direct users' tasks are investigated (focal tasks), the perceptions that the indirect users have about how tasks are performed are carefully considered when the performance metrics for each task are determined. The initial system design must explicitly support these focal tasks.

This design approach exercises the 80/20 rule that allows developers and designers to focus their efforts on the 20% of the tasks that users perform 80% of the time, leaving the remaining tasks to subsequent development spirals. This approach allows these teams to quickly develop the system, and lets the users assess the usefulness of the system by allowing them to focus on *their* primary tasks. If an element of a system designed using this model does not prove to be useful, it is unlikely that devoting additional time and money to develop the remaining 80% of the tasks performed only 20% of the time would be any more useful (or successful). In this way, employing user task analysis allows the UCD process to serve as a risk management function.

SSC CHARLESTON FINDINGS, ANALYSIS, AND RECOMMENDATIONS

Human factors engineering and HSI experts from SSC Charleston performed a pre-design analysis to determine the functional user requirements (FURs) necessary to design and upgrade an AT/FP Operations Center.

APPROACH

SSC Charleston used two approaches to integrate HSI best practices in the design and upgrade of AT/FP Operations Centers. The first approach was a pre-design analysis methodology that derived FURs that were subsequently used to drive the design of the facilities, systems, and tools of an AT/FP Operations Center. Therefore, the facilities, systems, and tools designed or selected had complete justification and traceability. The second approach was a traditional post-design methodology of site observation and interviews with Operations Center watchstanders.

For the pre-design methodology, the investigators detailed a FUR analysis methodology that was used for the Commander Navy Region Southeast (CNRSE) ROC/RDC pilot project. Although the SSC Charleston study was directed specifically towards the implementation of a regional AT/FP ROC/RDC concept, the methodology can be readily adapted to Operations Centers of various scope and complexity. The FUR approach is the up-front analysis required to derive and ensure incorporation of all relevant mission, functional, and user requirements into Operations Center design.

Functional User Requirements (FUR) Analysis in Operations Center Design

Develop Operational Capabilities

The first phase in the FUR approach is development of operational capabilities. Developing operational capabilities is the process of distilling user requirements from the applicable Navy Mission Essential Tasks (NMETs) and AT/FP capability areas. In this project, the investigators derived ROC NMETs by reviewing the capability areas supported by ROCs.

Derive ROC Mission-Essential Tasks

Table 2 lists the AT/FP capability areas that the ROC/RDC must support.

The NMETs are the supporting tasks required to enable the AT/FP mission through the Navy capability areas. Table 3 identifies the NMETS required to fulfill the eight capability areas addressed by the ROC in support of the AT/FP mission and operating model. From this list, the investigators proceeded to define the ROC mission-essential tasks, which are provided in Table 4.

Table 2. Capability areas supported by ROC.

		Regional Operations Center
CAPABILITIES	Reconnaissance	
	Early Warning	x
	Security Surveillance	
	Medical Surveillance	
	Inspections	
	Access Control	
	CBRN Detection	
	Explosives Detection	
	Attack Assessment	x
	Decision Making System	x
	C4I	x
	Operations Center	x
	Area Wide Alert/Notification	x
	CBRN Protection	
	Counter-Bomber	
	Blast Mitigation	
	Intrusion Response	
	Medical Response	x
	Air Defense	
	Waterside Protection	
	CBRNE Response	x
	CBRNE Recovery	

Table 3. NMET requirements mapped to ROC capabilities.

NTA	Task	Capability Area within ROC Concept
1	Deploy/Conduct Maneuvers	
2	Develop Intelligence	
2.1	Plan and Direct Intelligence Operations	
2.2	**Collect Data and Intelligence**	**Early Warning**
2.3	Process/Exploit Information and Intelligence	
2.3.1	Conduct Technical Processing and Exploitation	
2.3.2	**Correlate Information**	**Attack Assessment**
2.4	Produce Intelligence	
2.4.1	Evaluate Information	
2.4.2	Integrate Information	
2.4.3	**Interpret Information**	**Ops Centers, Attack Assessment**
2.4.4	Analyze and Synthesize Information	
2.4.4.1	**ID Issues and Threats**	**Ops Centers, Decision Making Systems, Attack Assessment**
2.4.4.2	Define the Battle Space Environment	
2.4.4.3	**Evaluate the Battle Space Environment**	**Decision Making Systems, Attack Assessment**
2.4.4.4	Evaluate the Threat	
2.4.4.5	Determine the Enemy's COA	
2.4.5	Prepare Intelligence Products	
2.4.5.1	Provide Support to the Commander's Estimate	
2.4.5.2	Provide Intelligence to Develop the Situation	
2.4.5.3	**Provide I&W of Threat**	**Early Warning, AWAN**
2.4.5.4	Provide Intelligence Support to Force Protection	
2.4.5.5	Provide Intelligence Support to Targeting	
2.4.6	Provide Intelligence Support to Combat Assessment	
2.5	**Disseminate and Integrate Intelligence**	**Ops Centers, Decision Making Systems, AWAN**
2.5.1	Determine Form to be used in Disseminating Intelligence	
2.5.2	**Establish Secure and Rapid Dissemination Means**	**Ops Centers, AWAN**
2.6	Evaluate Intelligence Operations	
3	Employ Firepower	
4	Perform Logistics and Combat Service Support	
4.1	Arm	
4.2	Fuel	
4.3	Repair/Maintain	
4.4	Provide Personnel and Support	
4.5	Provide Transport	
4.6	Supply the Force	
4.7	Provide Civil Military Engineering Support	
4.8	Support Civil Affairs in the Area of Operations	
4.8.1	Support Peace Operations	
4.8.2	Suppport Staff	
4.8.3	**Provide Interagency Coordination**	**Ops Centers, C4I, Decision Making Systems, AWAN**
4.8.4	**Coordinate with NGOs**	**Ops Centers, C4I, Decision Making Systems, AWAN**
4.9	Train Forces and Personnel	
4.10	Perform Resource Management	
4.10.1	Provide for Real Estate Management	
4.10.2	Manage Contracts and Contract Personnel	
4.10.3	**Coordinate Base and Station Activities**	**Response**
4.11	Provide Operations Legal Advice	
4.12	Provide Health Services	
4.13	Conduct Recovery and Salvage	
4.14	Provide Support Services	

Table 3. NMET requirements mapped to ROC capabilities. (cont)

5	**Exercise Command and Control**	**Ops Centers, C4I**
5.1	Acquire, Process, Communicate and Maintain Status of Information	
5.1.1	**Communicate Information**	**Ops Centers, C4I, AWAN, Response**
5.1.2	**Manage Means of Communicating Information**	**Ops Centers, C4I**
5.1.3	**Maintain Information and Naval Force Status**	**Ops Centers, C4I**
5.1.3.1	**Maintain and Display Tactical Picture**	**Ops Centers, C4I, Decision Making Systems, Attack Assessment**
5.1.3.2	Maintain and Display Force Command and Coordination Status	
5.1.3.3	**Maintain and Display Unit Readiness**	**Ops Centers, C4I, Decision Making Systems**
5.2	Analyze and Assess the Situation	
5.2.1	Analyze the Mission and Current Situation	
5.2.1.1	**Review and Evaluate the Situation**	**Ops Centers, Decision Making Systems, Attack Assessment, Response**
5.2.1.2	**Review and Evaluate Mission Guidance**	**Ops Centers, Decision Making Systems**
5.2.1.3	**Review the Rules of Engagement**	**Ops Centers, Decision Making Systems**
5.3	**Determine and Plan Actions and Operations**	**Ops Centers, Decision Making Systems**
5.3.1	Develop CONOPS	
5.3.1.1	Define Mission in Commanders Terms	
5.3.1.2	Provide CONOPS	
5.3.1.3	Develop Requirements and Priorities	
5.3.1.4	**Develop Procedures**	**Ops Centers, Decision Making Systems**
5.3.2	**Issue Plans and Guidance**	**Ops Centers**
5.3.3	**Develop COAs**	**Ops Centers, Decision Making Systems**
5.3.4	Analyze and Compare COAs	
5.3.5	Select/Modify COAs	
5.3.6	**Prioritize Subordinate Commander Requirements**	**Ops Centers, C4I**
5.3.7	Establish Force Command and Control Policy	
5.3.8	Issue Tactical Communications Estimate	
5.3.9	**Prepare Plans/Orders**	**Ops Centers, Decision Making Systems**
5.3.9.1	**Formulate Standing Plans**	**Ops Centers, Decision Making Systems**
5.3.9.2	**Develop Contingency Responses**	**Ops Centers, Decision Making Systems**
5.4	Direct, Lead and Coordinate Forces	
5.4.1	Direct Forces	
5.4.1.1	**Issue Orders**	**Ops Centers, C4I**
5.4.1.2	**Exercise Tactical Command and Control**	**Ops Centers, C4I**
5.4.2	Lead Forces	
5.4.3	Synchronize Tactical Ops and Integrate Maneuvers within Firepower	
5.4.4	Establish Liaisons	
5.4.5	**Report and Analyze Mission Readiness**	**Ops Centers**
5.5	Conduct Information Warfare	
5.6	Conduct Acoustic Warfare	
5.7	Establish Task Force HQ	
5.8	Provide PA Services	

Table 3. NMET requirements mapped to ROC capabilities. (cont)

6	Protect the Force	
6.1	Enhance Survivability	
6.1.1	Protect Against Combat Area Hazards	
6.1.1.1	**Protect Individuals and Systems**	**C4I, Decision Making Systems**
6.1.1.2	**Remove Hazards**	**Response**
6.1.1.3	Positively ID Friendly Forces	
6.1.2	Coordinate Perception Mgmt	
6.1.3	Conduct Counter-Deception	
6.1.4	Conduct Counter-Propaganda Operations	
6.1.5	Maintain Counter-Reconnaissance	
6.2	**Rescue and Recover**	**Response**
6.3	**Provide Security for Operational Forces and Means**	**C4I, Response**
6.3.1	Protect and Secure Area of Operations	
6.3.1.1	Establish and Maintain Rear Area Security	
6.3.1.2	Protect/Secure Operationally Critical Installtions, Facilities, Systems	
6.3.1.3	Provide Harbor Defense and Port Security	
6.3.1.4	Protect Lines of Communication	
6.3.1.5	**Establish and Enforce Protection Perimeter**	**Response**
6.3.1.6	Conduct Surveillance Detection Operations	
6.3.2	Conduct Military LE Support	
6.3.2.1	Manage Enemy Prisoners of War	
6.3.2.2	**Maintain Law and Order**	**Response**
6.3.2.3	Manage Refugees and Refugee Camps	
6.3.3	**Combat Terrorism**	**C4I, Decision Making Systems**
6.5	Perform Consequence Mgmt	
6.5.1	**Provide Disaster Relief**	**Response**
6.5.2	**Coordinate Damage Control Operations**	**Response**
6.5.3	**Provide Emergency Assistance**	**Response**
6.6	Provide Operational Safety of Personnel and Equipment	

Table 4. ROC mission-essential tasks.

NTA	Task	Definition
2.2	**Collect Data and Intelligence**	Gather data, info and previously produced intel from all sources to satisfy identified requirements
2.3.2	**Correlate Information**	Associate and combine data on a single subject to improve the credibility of the info
2.4.3	**Interpret Information**	Determine significance of info and its affects on current intel estimates
2.4.4.1	**ID Issues and Threats**	Assess threats to friendly tactical forces. Assess potential issues ans sits that could impact US Nat'l Security within AOR
2.4.4.3	**Evaluate the Battle Space Environment**	Eval the physical and civil envrnmts of the battlespace in order to ID the impact of envrnmt on both friendly and enemy forces
2.4.5.3	**Provide I&W of Threat**	Provide early warning of impending hostile action in order to prevent surprise and reduce risk from enemy actions
2.5	**Disseminate and Integrate Intelligence**	Provide intel to commanders in a timely way and in an appropriate form using suitable means
2.5.2	**Establish Secure and Rapid Dissemination Means**	Create and maintain communications and information systems for the delivery of intel (both supply push and demand pull)
4.8.3	**Provide Interagency Coordination**	Coordinate all civil affairs with the appropriate US agencies
4.8.4	**Coordinate with NGOs**	Coordinate civil affairs with NGOs as appropriate
4.10.3	**Cooridnate Base and Station Activities**	Ensure performance of naval base and station actions to support fleet and other commands and units
5	**Exercise Command and Control**	Exercise authority and direction over assigned or attached forces to accomplish the mission
5.1.1	**Communicate Information**	Send and receive data in usable formats
5.1.2	**Manage Means of Communicating Information**	Direct, establish or control the instrmnts used to send/receive info and to use various comms nets and modes for send/receive
5.1.3	**Maintain Information and Naval Force Status**	Screen, circulate, store and display info in a form that supports decision making and the tactical picture
5.1.3.1	**Maintain and Display Tactical Picture**	Process (fuse/correlate/filter) and maintain (auto/manual) raw data and display image-bldg info as the tact pic for tact level SA
5.1.3.3	**Maintain and Display Unit Readiness**	Track and display info on Unit Readiness to include status on all materiel deficiencies and personnel limitations
5.2.1.1	**Review and Evaluate the Situation**	Review the general tact sit, including available tactical data, intel assessments, envrnmt conditions and other external info
5.2.1.2	**Review and Evaluate Mission Guidance**	Review the CDR's mission guidance and intent (obj, specified/implied tasks) to ID constraints to assumptions and relate to the tact sit
5.2.1.3	**Review the Rules of Engagement**	Determine limitations on tactical action based on Rules of Engagement
5.3	**Determine and Plan Actions and Operations**	Make estimates and decisions based on assigned/projected/implied tasks and to examine aspects of potential ops to determine acceptable risks
5.3.1.4	**Develop Procedures**	Establish common reporting and tactical procedures including development of comms plans
5.3.2	**Issue Plans and Guidance**	Provide naval task force planners with info to develop COAs including specified and implied tasks
5.3.3	**Develop COAs**	Define ops for completing the mission based on analysis of the mission and determination of feasibility with regard to several factors
5.3.6	**Prioritize Subordinate Commander Requirements**	Resolve asset request conflicts and, in such cases, determine allocation of assets for subordinate commanders
5.3.9	**Prepare Plans/Orders**	Complete written/oral comms that convey info that governs actions, including those in selected COAs
5.3.9.1	**Formulate Standing Plans**	Formulate those pre-planned actions that can be included as standing plans and to modify existing plans, as necessary
5.3.9.2	**Develop Contingency Responses**	Formulate immediate responses to threats that can be forseen or anticipated
5.4.1.1	**Issue Orders**	Guide and command the exec of plans inc plans for transmission to sub/support units for exec and to adj and higher units for coord/apprvl
5.4.1.2	**Exercise Tactical Command and Control**	Execute C2 (e.g., order warfare degrees of readiness, direct asset assignment, movement and employment, control tactical assets)
5.4.5	**Report and Analyze Mission Readiness**	Review data and produce routine, periodic, sit and status reports as well as reporting ability to continue mission following sig tact events
6.1.1.1	**Protect Individuals and Systems**	Use protective positions, measures or eqpmt to reduce the effects of enemy and friendly weapon systems and to enhance force effectiveness.
6.1.1.2	**Remove Hazards**	Eliminate the presence of hazards to equipment and personnel
6.2	**Rescue and Recover**	Rescue and recover military and civilian personnel, equipment and systems
6.3	**Provide Security for Operational Forces and Means**	Enhance freedom of action by identifying and reducing friendly vulnerabilities to hostile acts, influence or surprise
6.3.1.5	**Establish and Enforce Protection Perimeter**	Establish a force protection perimeter
6.3.2.2	**Maintain Law and Order**	Enforce laws and regs and maintain the discipline of personnel inc LE, criminal invest, counter-drug act, CT and assisting US civil authorities
6.3.3	**Combat Terrorism**	Perform def and off measures to reduce vulnerability of individuals and property to terrorist acts; to prevent deter and respond to terrorism
6.5.1	**Provide Disaster Relief**	Deliver disaster relief, inc personnel and supplies, and provide a mobile, flexible, rapidly responsive medical capability
6.5.2	**Coordinate Damage Control Operations**	Perform all necessary actions required to respond to and fight all port and base fires, casualties and other damage
6.5.3	**Provide Emergency Assistance**	Perform all necessary actions required to assist in responding to enemy attack or natural incident

Organization of ROC within NMETs

The previous subsection outlined the derivation of the specific tasks that must be completed by the ROC to fulfill its high-level mission within AT/FP. Although NMETs outline a comprehensive list of tasking to be completed by the ROC, it is difficult to envision how each task relates to the ROC operating picture. Functional concepts needed within the ROC begin to emerge when the tasks are grouped together based on similar traits.

Grouping the NMETs

Organizing tasks within NMETs based on similar functionality leads to the development of four functional concepts addressed by the ROC-specific NMETs. The following subsections identify and explain each functional concept. The functional concepts include the following:

- Proactive Analysis and Coordination
- Reactive Analysis and Coordination
- Emergency Response
- Communications Support

Proactive Analysis and Coordination

The Proactive Analysis and Coordination concept works within the detection and assessment periods of the AT/FP operating model. It consists of two proactive functions that include the following:

- **Intelligence Monitoring.** Gather intelligence and information regarding threats to Navy critical assets from different federal agencies (including the Department of Homeland Security) and assess gathered information and support planning and decisions of decision-makers. This function is not responsible for actively collecting or developing intelligence. Rather, it acts as the Navy's regional primary means for information coordination.
- **Sensor Monitoring.** Watch sensors are at bases throughout the region. Every Navy installation operates event-driven alarms, and these alarms must be monitored 24/7, allowing the ROC to detect possible threats.

Table 5 lists the NMETs addressed within the Proactive Analysis and Coordination concept. The highlighted sections of the table represent tasks that affect multiple functional concepts.

Table 5. NMETs addressed within the Proactive Analysis and Coordination concept.

NTA	TASK
2.2	Collect Data and Intelligence
2.3.2	Correlate Information
2.4.3	Interpret Information
2.4.4.1	ID Issues and Threats
2.4.4.3	Evaluate the Battle Space Environment
2.4.5.3	Provide I&W of Threat
2.5	Disseminate and Integrate Intelligence
2.5.2	Establish Secure and Rapid Dissemination Means
4.8.3	Provide Interagency Coordination
4.8.4	Coordinate with NGOs
4.10.3	Cooridnate Base and Station Activities

Reactive Analysis and Coordination

The Reactive Analysis and Coordination concept is active during the defense and recovery periods of the AT/FP operating model. It consists of one reactive function:

- **Emergency Management.** This measure is responsible for developing and delivering situation awareness (SA) to key decision-making systems at the ROC during crisis situations. It combines information and intelligence gathered by separate installations regarding a given incident and is heavily involved in decision-making support.

Table 6 lists the NMETs addressed within the Reactive Analysis and Coordination concept. The highlighted sections of the chart represent tasks that affect multiple functional concepts.

Table 6. NMETs addressed within the Reactive Analysis and Coordination concept.

NTA	TASK
4.8.3	Provide Interagency Coordination
4.8.4	Coordinate with NGOs
4.10.3	Cooridnate Base and Station Activities
5	Exercise Command and Control
5.1.3	Maintain Information and Naval Force Status
5.1.3.1	Maintain and Display Tactical Picture
5.1.3.3	Maintain and Display Unit Readiness
5.2.1.1	Review and Evaluate the Situation
5.2.1.2	Review and Evaluate Mission Guidance
5.2.1.3	Review the Rules of Engagement
5.3	Determine and Plan Actions and Operations
5.3.1.4	Develop Procedures
5.3.2	Issue Plans and Guidance
5.3.3	Develop COAs
5.3.6	Prioritize Subordinate Commander Requirements
5.3.9	Prepare Plans/Orders
5.3.9.1	Formulate Standing Plans
5.3.9.2	Develop Contingency Responses
5.4.5	Report and Analyze Mission Readiness

Emergency Response

The Emergency Response concept is active 24/7/365, but its main role is carried out during the defense period of the AT/FP operating model. It is responsible for providing SA to decision-making systems and deploying and supporting Emergency Response. It consists of one response support function:

- **Emergency Response.** Emergency Response includes the dispatching measure of directing emergency responders to the points of need and providing a communication line between emergency responders and ROC decision-makers. This concept extends the level of SA available to incident decision-makers by allowing on-scene responders to convey ground-level information regarding an incident to the ROC.

Table 7 lists the NMETs addressed within the Emergency Response concept.

Table 7. NMETs addressed within the Emergency Response concept.

NTA	TASK
6.1.1.1	Protect Individuals and Systems
6.1.1.2	Remove Hazards
6.2	Rescue and Recover
6.3	Provide Security for Operational Forces and Means
6.3.1.5	Establish and Enforce Protection Perimeter
6.3.2.2	Maintain Law and Order
6.3.3	Combat Terrorism
6.5.1	Provide Disaster Relief
6.5.2	Coordinate Damage Control Operations
6.5.3	Provide Emergency Assistance

Communications Support

The Communications Support concept is responsible for ensuring communication connectivity among different entities responsible for accomplishing the ROC-specific NMETs. Table 8 lists the NMETs addressed within the Communications Support concept.

Table 8. NMETs addressed within the Communications Support concept.

NTA	TASK
5.1.1	Communicate Information
5.1.2	Manage Means of Communicating Information

Mapping ROC NMETs to Functional Concepts

The next step in the process is to associate ROC NMETs to the functional concepts discussed above. Table 9 maps the four functional concepts identified above to the tasks listed in the NMETs for the ROC.

ROC Functional Areas

To support the missions identified by AT/FP, the ROC must accomplish the tasks defined in Table 3. After organizing the NMETs into the four ROC functional concepts illustrated in Tables 5 through 8, five functional areas that carry out the AT/FP mission-essential tasks were identified:

- Planning, Intelligence, and Assessment
- Sensor Monitoring
- Emergency Management Command and Control
- Emergency Response (Dispatch)
- Communications

Table 9. Four functional concepts mapped to ROC NMET tasks.

NTA	Task	Proactive Analysis & Coordination	Reactive Analysis & Coordination	Emergency Response & Support	Communication Support
2.2	Collect Data and Intelligence	x			
2.3.2	Correlate Information	x			
2.4.3	Interpret Information	x			
2.4.4.1	ID Issues and Threats	x			
2.4.4.3	Evaluate the Battle Space Environment	x			
2.4.5.3	Provide I&W of Threat	x			
2.5	Disseminate and Integrate Intelligence	x			
2.5.2	Establish Secure and Rapid Dissemination Means	x			
4.8.3	Provide Interagency Coordination	x	x		
4.8.4	Coordinate with NGOs	x	x		
4.10.3	Cooridnate Base and Station Activities	x	x		
5	Exercise Command and Control		x		
5.1.1	Communicate Information				x
5.1.2	Manage Means of Communicating Information				x
5.1.3	Maintain Information and Naval Force Status		x		
5.1.3.1	Maintain and Display Tactical Picture		x		
5.1.3.3	Maintain and Display Unit Readiness		x		
5.2.1.1	Review and Evaluate the Situation		x		
5.2.1.2	Review and Evaluate Mission Guidance		x		
5.2.1.3	Review the Rules of Engagement		x		
5.3	Determine and Plan Actions and Operations		x		
5.3.1.4	Develop Procedures		x		
5.3.2	Issue Plans and Guidance		x		
5.3.3	Develop COAs		x		
5.3.6	Prioritize Subordinate Commander Requirements		x		
5.3.9	Prepare Plans/Orders		x		
5.3.9.1	Formulate Standing Plans		x		
5.3.9.2	Develop Contingency Responses		x		
5.4.1.1	Issue Orders				
5.4.1.2	Exercise Tactical Command and Control				
5.4.5	Report and Analyze Mission Readiness		x		
6.1.1.1	Protect Individuals and Systems			x	
6.1.1.2	Remove Hazards			x	
6.2	Rescue and Recover			x	
6.3	Provide Security for Operational Forces and Means			x	
6.3.1.5	Establish and Enforce Protection Perimeter			x	
6.3.2.2	Maintain Law and Order			x	
6.3.3	Combat Terrorism	x	x	x	
6.5.1	Provide Disaster Relief			x	
6.5.2	Coordinate Damage Control Operations			x	
6.5.3	Provide Emergency Assistance			x	

Planning, Intelligence, and Assessment (PIA)

The ROC PIA function is present 24/7 in the ROC and collects multiple-source intelligence, analyzes this information, and provides information assessments. These assessments are immediately passed to key leadership in the appropriate formats to provide SA information to decision-makers.

PIA supports ROC emergency management and emergency dispatch by providing SA updates to the regional commander and appropriate external entities. The function also supports ROC leadership components in command evaluation and elevations of issues to the Regional Commander.

Sensor Monitoring

The ROC Sensor Monitoring function provides 24/7 monitoring of critical regional feeds in support of ROC C2. This function supports the RDC 24/7 by providing information on triggered sensors that require an Emergency Response to be dispatched. During crisis situations, the sensor monitoring function supports the ROC through the provision of SA to personnel involved in regional AT/FP.

Emergency Management Command and Control (EMC2)

The ROC EMC2 function is the event-driven emergency management function. In response to a regional incident, the EMC2 function manages regional incidents/events of varying scale and is the C2 point of regional (multi-base) resources for incident management. It is “dark” (unmanned) during routine operations and an isolated base-level incident, and “light” (manned) during multi-base incidents and large-scale national incidents.

The ROC EMC2 function is composed of four groups:

- **Operations.** Develops tactical objectives and conducts tactical operations to carry out the action plan. Organizes personnel and directs resources in response to an incident.
- **Planning.** Develops the action plan to accomplish the objectives. Collects and evaluates relevant information. Maintains the status of resources available to the Emergency Response team.
- **Logistics.** Provides support to meet incident needs. Incident needs include resources and other services needed to support the response plan to an incident.
- **Financial/Administrative.** Monitors costs related to an incident, provides accounting services, tracks procurement time, and performs cost analysis.

Emergency Response Dispatch

The ROC Emergency Response Dispatch function provides regionalized 911 call and dispatch for police, fire, and emergency medical services. It also provides SA support to the ROC by acting as an information node. It is involved in 24/7 operations within the ROC.

Communications

The ROC Communications function provides all necessary communications patching and support between ROC leadership, the regional commander, and appropriate external entities. It supports emergency management, emergency dispatch, and 24/7 operations within the ROC.

MAPPING ROC FUNCTIONAL AREAS TO THE ROC NMETs

Mapping the functional capability areas to the mission-essential tasks is the final piece in deriving operational capabilities for the ROC. Table 10 links the specific functional capability areas to the AT/FP vision by identifying the specific tasks for which each functional capability area is responsible.

OPERATIONAL CAPABILITIES SUMMARY

Analysis of the functional areas mapped to the ROC NMETs provided the operational capability needs for a ROC/RDC. Navy ROC/RDC NMETs were identified within AT/FP ROC/RDC-specific capability areas and aligned with the operating model to provide a more complete operational breakdown of the AT/FP vision. The operational breakdown uncovered three areas in which the ROC/RDC must operate to effectively accomplish the higher level AT/FP vision. The three areas are Proactive, Reactive, and Supporting Operations. The operating areas break down further into five functional capability areas required at the ROC/RDC to achieve the 41 ROC/RDC-specific NMETs. Figure 9 provides an overview of this breakdown, including the identified five functional capability areas present at the ROC/RDC.

The next phase in the FUR approach was to derive system capacities. In this phase, SSC Charleston first defined user roles and responsibilities and then began to identify systems and tools that users could use to implement ROC/RDC operational capabilities.

DEFINE USER ROLES AND RESPONSIBILITIES

The ROC/RDC requires on-site personnel to accomplish many of the mission-driven tasks mapped out in ROC/RDC NMETs. The ROC/RDC, as described earlier, must complete its mission during 24/7 operations and incident-triggered operations. Each operation is completed by personnel present at the ROC/RDC 24/7 or personnel present solely during incident situations.

The following user roles and responsibilities were derived from NMETs, AT/FP CONOPS, and National Interagency Incident Management System Incident Command System documentation.

24/7 Operations

The personnel identified below are involved in 24/7 operations at the ROC/RDC, regardless of the situation. During incident and non-incident situations, they provide situational support to AT/FP support personnel. Many of these personnel are also responsible for increasing the protection of military assets by quickly directing response to emergencies.

- ROC Watch Officer
- Assistant Watch Officer
- Sensor Operator
- Dispatch Manager
- Dispatch Supervisor
- Dispatcher
- Communications Operator

Table 10. ROC functional areas mapped to ROC NMETs.

NTA	Task	ROC Functional Area
2.2	Collect Data and Intelligence	PIA, Sensor Monitoring
2.3.2	Correlate Information	PIA, Sensor Monitoring
2.4.3	Interpret Information	PIA, Sensor Monitoring
2.4.4.1	ID Issues and Threats	PIA, Sensor Monitoring
2.4.4.3	Evaluate the Battle Space Environment	PIA, Sensor Monitoring
2.4.5.3	Provide I&W of Threat	PIA, Sensor Monitoring
2.5	Disseminate and Integrate Intelligence	PIA
2.5.2	Establish Secure and Rapid Dissemination Means	PIA
4.8.3	Provide Interagency Coordination	PIA,C2
4.8.4	Coordinate with NGOs	PIA, C2
4.10.3	Cooridnate Base and Station Activities	PIA, C2
5	Exercise Command and Control	C2
5.1.1	Communicate Information	COMMS
5.1.2	Manage Means of Communicating Information	COMMS
5.1.3	Maintain Information and Naval Force Status	C2
5.1.3.1	Maintain and Display Tactical Picture	C2
5.1.3.3	Maintain and Display Unit Readiness	C2
5.2.1.1	Review and Evaluate the Situation	C2
5.2.1.2	Review and Evaluate Mission Guidance	C2
5.2.1.3	Review the Rules of Engagement	C2
5.3	Determine and Plan Actions and Operations	C2
5.3.1.4	Develop Procedures	C2
5.3.2	Issue Plans and Guidance	C2
5.3.3	Develop COAs	C2
5.3.6	Prioritize Subordinate Commander Requirements	C2
5.3.9	Prepare Plans/Orders	C2
5.3.9.1	Formulate Standing Plans	C2
5.3.9.2	Develop Contingency Responses	C2
5.4.1.1	Issue Orders	
5.4.1.2	Exercise Tactical Command and Control	
5.4.5	Report and Analyze Mission Readiness	C2
6.1.1.1	Protect Individuals and Systems	Dispatch
6.1.1.2	Remove Hazards	Dispatch
6.2	Rescue and Recover	Dispatch
6.3	Provide Security for Operational Forces and Mean	Dispatch
6.3.1.5	Establish and Enforce Protection Perimeter	Dispatch
6.3.2.2	Maintain Law and Order	Dispatch
6.3.3	Combat Terrorism	PIA, C2, Sensor Monitoring, Dispatch
6.5.1	Provide Disaster Relief	Dispatch
6.5.2	Coordinate Damage Control Operations	Dispatch
6.5.3	Provide Emergency Assistance	Dispatch

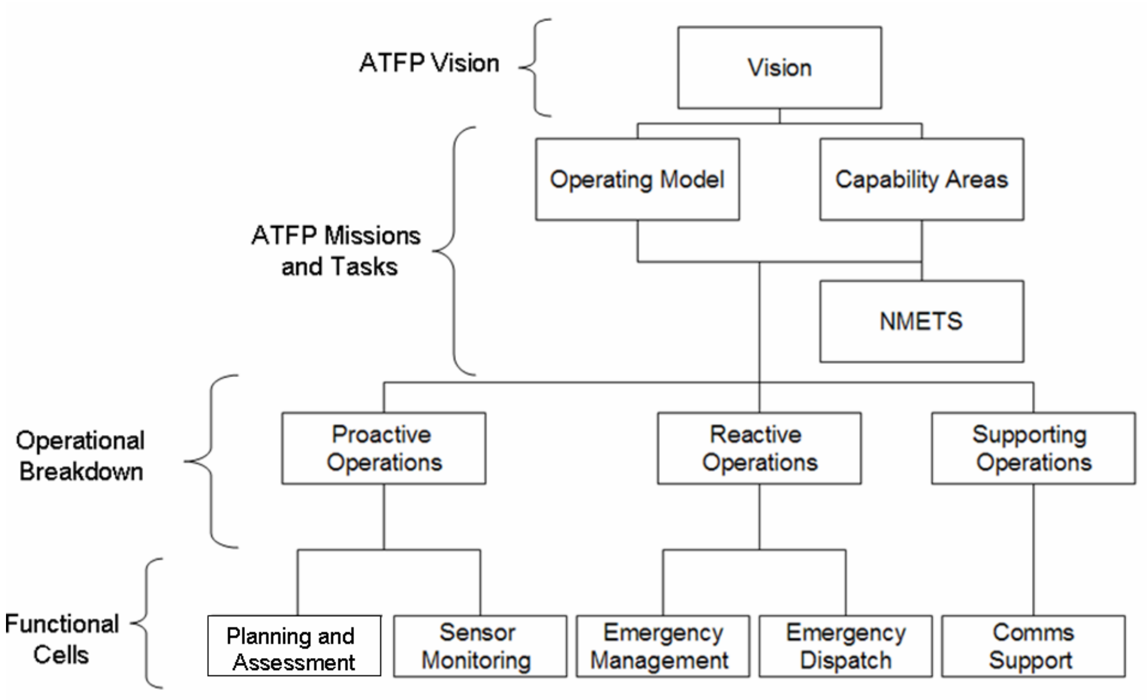

Figure 9. Overview of the five ROC/RDC functional capability areas.

Incident Command System Operations

The following personnel are responsible for handling emergency management. These personnel are only active during incidents and are not present during 24/7 operations.

- Command Duty Officer
- Public Information Officer
- Safety Officer
- Liaison Officer
- Staff Judge Advocate
- Operations Section Officer
- Planning and Intelligence Section Officer
- Logistic Section Officer
- Finance and Administration Section Officer

MAPPING FUNCTIONAL AREAS TO USERS

Table 11 maps each of the previously defined users to a ROC functional area.

Table 11. Users mapped to ROC functional areas.

		Planning and Intel	C2	Sensor Monitoring	Communications	Dispatch
24x7 Operations	Watch Officer	x				
	Watch Assistant	x				
	Dispatch Manager					x
	Dispatch Supervisor					x
	Dispatcher					x
	Sensor Operator			x		
	Communications Operators				x	
Incident Command System	Director	x				
	Public Information Officer	x				
	Safety Officer	x				
	Liaison Officer	x				
	Staff Judge Advocate	x				
	Operations Section Officer		x			
	Planning and Intel Officer		x			
	Logistics Section Officer		x			
	Finance and Administrative Officer		x			

ROC/RDC SYSTEMS AND APPLICATIONS

The following systems—both current and proposed—support (or will be required to support) the ROC/RDC functional areas as they perform the tasks supporting the AT/FP mission.

Area Security Operations C2 System (ASOCC)

WebEOC (a Web-based emergency management system)

Joint Protection Information Exchange System (JRIES)

Joint Protection Enterprise Network (JPEN)

Global C2 Systems (GCCS)

Local SA System (LSAS)

Defense Message System (DMS)

Enterprise Land Mobile Radio (E-LMR)

Computer-Aided Dispatch (CAD)

Chemical Biological Radiological Nuclear Explosives (CBRNE)

Force Protection Tactical Decision Aid (TDA)

Infrared

Meridian Digital Centrex

Navy Emergency Response Management System (NERMS)

Non-Secure Internet Protocol Router (NIPRNET)

Navy and Marine Corps Intranet (NMCI)

Record Management System

Secure Internet Protocol Router

Unmanned Aerial Vehicle

ROC/RDC SYSTEM CAPABILITY MATRIX

The capability matrix in Table 12 maps ROC support systems to the ROC/RDC functional areas.

Table 12. ROC/RDC system capability matrix.

	FUNCTIONAL AREAS				
ROC SUPPORT SYSTEMS	PLANNING INTEL AND ASSESSMENT	C2 CELL	SENSOR MONITORING	COMMUNICATIONS	DISPATCH
Radar			x		
Access Control Automated Alarms					x
Area Secure Operations Command and Control	x	x			
Computer Aided Dispatch					x
Chemical Biological Radiological Nuclear Explosives					x
Defense Messaging System	x				x
Enterprise Land Mobile Radio					x
Federal Emergency Management Administration		x			
Force Protection Tactical Decision Aid					x
Global Command & Control System	x				
Information Management Pilot Program	x	x	x		
Infra-Red			x		
Joint Protection Enterprise Network	x				
Joint Regional Information Exchange System	x	x			
Land Status Automated System	x				
Meridian Digital Centrex					x
Navy Emergency Response Management System					x
Non-secure Internet Protocol Router	x	x		x	
Nuclear Information Suppliers System [swimmers?]			x		
Navy and Marine Corps Intranet	x	x	x	x	x
Public Telephone & Telegraph				x	
Records Management System					x
Satellite Communications				x	
Secure Internet Protocol Router	x	x		x	
Unmanned Aerial Vehicle			x		
Video Tele-Conferencing			x		
Web-Emergency Operations Center Link	x				

EQUIPMENT FORECAST

Based on the roles and responsibilities of the users defined in the previous subsection, the operational intent outlined by the Operational Capabilities Demonstration (OCD), and the systems to be implemented at the ROC/RDC, an equipment forecast for each functional cell is provided in the following subsections. Tables 13 through 21 support the ROC/RDC operational intent defined in the OCD.

Planning and Assessment Cell

The following subsections define a Desired Equipment Forecast and Minimal Equipment Forecast for each workstation on the floor.

Desired Capability

The desired capabilities for each personnel workstation within the Planning and Assessment (PA) Cell are listed below. These desired capabilities are based on implemented system requirements and personnel requirements.

- Offices are dedicated to the Regional Emergency Manager, the Deputy Regional Emergency Manager, and the Chemical Biological Nuclear Radiological and Explosives Officer.
- Office positions must have access to classified as well as unclassified information.
- Office positions must have the capability of switching their visual display (a dual-monitor display) from a classified PC to an unclassified PC and display both classified and unclassified information simultaneously.
- The primary function of the Regional Commander Staff support positions is to provide the regional commander with information regarding specific areas of expertise and to notify the public and related federal, state, and local agencies of relevant information regarding an incident.

Desired Hardware Capacity Matrix

Table 13. Desired Hardware Capacity Matrix for PA Cell.

	SEAT	USERS	NMCI SEAT TYPE RED	NMCI SEAT TYPE WHITE	NMCI SEAT TYPE BLUE	NMCI SEAT TYPE S&T	UNCLASS LAN	CLASS LAN	OTHER LAN	UNCLASS PCs	CLASS PCs	MONITORS	KVM SWITCH	MICE	KEYBOARDS	LAPTOPS	LAPTOP FEEDS	UNCLASS PHONES	CLASS PHONES	OTHER PHONES	SPEAKERS	HEADSET	VTC	VIDEO DISPLAY	SCANNERS	UNCLASS FAX	CLASS FAX	WHITEBOARD	COPIERS	UNCLASS B&W PRINTERS	CLASS B&W PRINTER	UNCLASS COLOR PRINTERS	CLASS COLOR PRINTER	SHREDDERS	UPS	UNCLASS RACKS	CLASS RACKS
REGIONAL OPERATIONS CENTER																																					
EXECUTIVE LEADERSHIP / PLANNING & ASSESSMENT CELL																																					
OFFICE PERSONNEL																																					
ROC.REM.01 (Emergency Mgr Office)	1	1				1	1	1		1	1	2	1	1	1			1	1		1			1				1				1	1		2		
ROC.DREM.01 (Dep Emergency Mgr Office)	1	1				1	1	1		1	1	2	1	1	1			1	1		1			1				1				1	1		2		
ROC.CBRNE.S.01 (CBRE Support Office)	1	1				1	1	1		1	1	2	1	1	1			1	1		1							1				1	1		2		
FLOOR PERSONNEL																																					
ROC.PA.RC.01 (Regional Commander WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.CDO.01 (CDO WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.STAFF.01 (SJA WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.STAFF.02 (SAFE at Table)	1	1															1	1																			
ROC.PA.STAFF.03 (PIO at Table)	1	1															1																				
ROC.PA.STAFF.04 (LO at Table)	1	1															1																				
ROC.PA.SWO.01 (Watch Officer WS)	1	5				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.ASWO.01 (Assistant WO WS)	1	5				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.SUPPORT.01 (COMM Operator WS)	1	5				1	1	1		1	1	2	1	1	1			1	1			1													2		
SUPPORT AREA																																					
PA SUPPORT ZONE							1	1																	1	1	1	1	1	1	1	1	1	1			
EXEC / PA CELL TOTALS	12	24	0	0	0	9	10	10	0	9	9	18	9	9	9	0	3	10	9	0	3	6	0	2	1	1	1	4	1	1	1	4	4	1	15	0	0

Minimum Acceptable Hardware Capacity Matrix

Table 14. Minimum Acceptable Hardware Capability Matrix for PA cell.

	SEAT	USERS	NMCI SEAT TYPE RED	NMCI SEAT TYPE WHITE	NMCI SEAT TYPE BLUE	NMCI SEAT TYPE S&T	UNCLASS LAN	CLASS LAN	OTHER LAN	UNCLASS PCs	CLASS PCs	MONITORS	KVM SWITCH	MICE	KEYBOARDS	LAPTOPS	LAPTOP FEEDS	UNCLASS PHONES	CLASS PHONES	OTHER PHONES	SPEAKERS	HEADSET	VTC	VIDEO DISPLAY	SCANNERS	UNCLASS FAX	CLASS FAX	WHITEBOARD	COPIERS	UNCLASS B&W PRINTERS	CLASS B&W PRINTER	UNCLASS COLOR PRINTERS	CLASS COLOR PRINTER	SHREDDERS	UPS	UNCLASS RACKS	CLASS RACKS
REGIONAL OPERATIONS CENTER																																					
EXECUTIVE LEADERSHIP / PLANNING & ASSESSMENT CELL																																					
OFFICE PERSONNEL																																					
ROC.REM.01 (Emergency Mgr Office)	1	1				1	1	1		1	1	2	1	1	1			1	1		1							1				1	1		2		
ROC.DREM.01 (Dep Emergency Mgr Office)	1	1				1	1	1		1	1	2	1	1	1			1	1		1							1				1	1		2		
ROC.CBRNE.S.01 (CBRE Support Office)	1	1				1	1			1		2		1	1			1			1							1				1			2		
FLOOR PERSONNEL																																					
ROC.PA.RC.01 (Regional Commander WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.CDO.01 (CDO WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.STAFF.01 (SJA WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.STAFF.02 (SAFE at Table)	1	1															1	1																			
ROC.PA.STAFF.03 (PIO at Table)	1	1																																			
ROC.PA.STAFF.04 (LO at Table)	1	1																																			
ROC.PA.SWO.01 (Watch Officer WS)	1	5				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.ASWO.01 (Assistant WO WS)	1	5				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.PA.SUPPORT.01 (COMM Operator WS)	1	5				1	1	1		1	1	2	1	1	1			1	1			1													2		
SUPPORT AREA																																					
PA SUPPORT ZONE																																					
EXEC / PA CELL TOTALS	12	24	0	0	0	9	9	8	0	9	8	18	8	9	9	0	1	10	8	0	3	6	0	0	0	0	0	3	0	0	0	3	2	0	15	0	0

Sensor Monitoring Cell

Table 15. Sensor monitoring cell.

	SEAT	USERS	NMCI SEAT TYPE RED	NMCI SEAT TYPE WHITE	NMCI SEAT TYPE BLUE	NMCI SEAT TYPE S&T	UNCLASS LAN	CLASS LAN	OTHER LAN	UNCLASS PCs	CLASS PCs	MONITORS	KVM SWITCH	MICE	KEYBOARDS	LAPTOPS	LAPTOP FEEDS	UNCLASS PHONES	CLASS PHONES	OTHER PHONES	SPEAKERS	HEADSET	VTC	VIDEO DISPLAY	SCANNERS	UNCLASS FAX	CLASS FAX	WHITEBOARD	COPIERS	UNCLASS B&W PRINTERS	CLASS B&W PRINTER	UNCLASS COLOR PRINTERS	CLASS COLOR PRINTER	SHREDDERS	UPS	UNCLASS RACKS	CLASS RACKS
SENSOR MONITORING CELL																																					
FLOOR PERSONNEL																																					
RDC.SM.O.01 (Sensor Monitoring WS)	1	5				?	?	?	?	?	?	?	?	?	?			?	?	?	?	?		?											?		
RDC.SM.O.02 (Sensor Monitoring WS)	1	5				?	?	?	?	?	?	?	?	?	?			?	?	?	?	?		?											?		
RDC.SM.O.03 (Sensor Monitoring WS)	1	5				?	?	?	?	?	?	?	?	?	?			?	?	?	?	?		?											?		
SUPPORT AREA																																					
SENSOR MONITORING SUPPORT ZONE																																					
SENSOR MONITORING CELL TOTALS	3	15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Emergency Management Command and Control Cell

The desired capabilities for each personnel workstation within the Emergency Management Command and Control (EMC2) Cell are listed in the following subsections.

Desired Capability and Assumptions

These desired capabilities are based on implemented system requirements and personnel requirements.

- All applications needed within the EMC2 Cell are Web-portal-based.
- All section officers (Planning and Intelligence, Finance and Administrative, Logistics, Operations) are required to view both classified and unclassified information.

Desired System Capacity Matrix

Table 16. Desired System Capacity Matrix for the EMC2.

	SEAT	USERS	NMCI SEAT TYPE RED	NMCI SEAT TYPE WHITE	NMCI SEAT TYPE BLUE	NMCI SEAT TYPE S&T	UNCLASS LAN	CLASS LAN	OTHER LAN	UNCLASS PCs	CLASS PCs	MONITORS	KVM SWITCH	MICE	KEYBOARDS	LAPTOPS	LAPTOP FEEDS	UNCLASS PHONES	CLASS PHONES	OTHER PHONES	SPEAKERS	NON-USB HEADSET	VTC	VIDEO DISPLAY	SCANNERS	UNCLASS FAX	CLASS FAX	WHITEBOARD	COPIERS	UNCLASS B&W PRINTERS	CLASS B&W PRINTER	UNCLASS COLOR PRINTERS	CLASS COLOR PRINTER	SHREDDERS	UPS	UNCLASS RACKS	CLASS RACKS
EMERGENCY MANAGEMENT / C2 CELL																																					
FLOOR PERSONNEL																																					
ROC.EMC2.LFA.SO.01 (LFA Section Officer WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.LFA.01 (COMM Operator WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.LFA.02 (TECH Support WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.LFA.03 (LFA WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.LFA.04 (LFA WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.LFA.05 (LFA WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.LFA.06 (LFA WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.O.SO.01 (Ops Section Officer WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.O.01 (Ops WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.O.02 (Ops WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.O.03 (Ops WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.O.04 (Ops WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.O.05 (Ops WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.O.06 (Ops WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.PI.SO.01 (PI Section Officer WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.PI.01 (PI WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.PI.02 (PI WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.PI.03 (PI WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.PI.04 (PI WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.PI.05 (PI WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.PI.06 (PI WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
SUPPORT AREA																																					
EM / C2 COLLABORATION TABLE																																					
EM / C2 SUPPORT ZONE							1	1																	1	1	1	1		1	1	1	1	1			
EM / C2 CELL TOTAL	21	21	0	0	0	21	22	22	0	21	21	42	21	21	21	0	0	21	21	0	0	21	0	0	1	1	1	1	0	1	1	1	1	1	32	0	0

Minimum Acceptable Hardware Capacity Matrix

Table 17. Minimum Acceptable Hardware Capacity Matrix for the EMC2.

	SEAT	USERS	NMCI SEAT TYPE RED	NMCI SEAT TYPE WHITE	NMCI SEAT TYPE BLUE	NMCI SEAT TYPE S&T	UNCLASS LAN	CLASS LAN	OTHER LAN	UNCLASS PCs	CLASS PCs	MONITORS	KVM SWITCH	MICE	KEYBOARDS	LAPTOPS	LAPTOP FEEDS	UNCLASS PHONES	CLASS PHONES	OTHER PHONES	SPEAKERS	NON-USB HEADSET	VTC	VIDEO DISPLAY	SCANNERS	UNCLASS FAX	CLASS FAX	WHITEBOARD	COPIERS	UNCLASS B&W PRINTERS	CLASS B&W PRINTER	UNCLASS COLOR PRINTERS	CLASS COLOR PRINTER	SHREDDERS	UPS	UNCLASS RACKS	CLASS RACKS
EMERGENCY MANAGEMENT / C2 CELL																																					
FLOOR PERSONNEL																																					
ROC.EMC2.LFA.SO.01 (LFA Section Officer WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.LFA.01 (COMM Operator WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.LFA.02 (TECH Support WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.LFA.03 (LFA WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.LFA.04 (LFA WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.LFA.05 (LFA WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.LFA.06 (LFA WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.O.SO.01 (Ops Section Officer WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.O.01 (Ops WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.O.02 (Ops WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.O.03 (Ops WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.O.04 (Ops WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.O.05 (Ops WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.O.06 (Ops WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.PI.SO.01 (PI Section Officer WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.PI.01 (PI WS)	1	1				1	1	1		1	1	2	1	1	1			1	1			1													2		
ROC.EMC2.PI.02 (PI WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.PI.03 (PI WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.PI.04 (PI WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.PI.05 (PI WS)	1	1				1	1			1		2		1	1			1				1													2		
ROC.EMC2.PI.06 (PI WS)	1	1				1	1			1		2		1	1			1				1													2		
SUPPORT AREA																																					
EM / C2 COLLABORATION TABLE																																					
EM / C2 SUPPORT ZONE							1	1																	1	1	1	1		1	1	1	1	1			
EM / C2 CELL TOTAL	21	21	0	0	0	21	22	7	0	21	6	42	6	21	21	0	0	21	6	0	0	21	0	0	1	1	1	1	0	1	1	1	1	1	32	0	0

Dispatch Cell

The following subsections describe the desired capabilities for each personnel workstation within the Dispatch Cell.

Desired Capability and Assumptions

Desired capabilities are based on the following implemented system requirements and personnel requirements:

- The Dispatch Manager must have access to both classified and unclassified information in his/her office.
- The Dispatch Manager has the ability to sit on the dispatch floor to observe the work of dispatchers.
- The Dispatch Supervisor has the capability of performing the same tasks as any Dispatch Operator on the floor, and therefore must have the same desk configuration as all other Dispatch Operators on the floor.
- The Dispatch Supervisor and all Dispatch Operators on the floor have no classified connectivity requirement.
- The system, Enhanced Land Mobile Radio (ELMR) has a touch-screen desktop configuration. Therefore, ELMR does not require a mouse or keyboard. However, NERMS will require a mouse and keyboard.
- Because this cell is a 24/7 operational cell, five users must have access to each workstation to handle all working shifts.

Desired Hardware Capacity Matrix

Table 18. Desired Hardware Capacity Matrix.

	SEAT	USERS	NMCI SEAT TYPE RED	NMCI SEAT TYPE WHITE	NMCI SEAT TYPE BLUE	NMCI SEAT TYPE S&T	UNCLASS LAN	CLASS LAN	OTHER LAN	UNCLASS PCs	CLASS PCs	MONITORS	KVM SWITCH	MICE	KEYBOARDS	LAPTOPS	LAPTOP FEEDS	UNCLASS PHONES	CLASS PHONES	OTHER PHONES	SPEAKERS	HEADSET	VTC	VIDEO DISPLAY	SCANNERS	UNCLASS FAX	CLASS FAX	WHITEBOARD	COPIERS	UNCLASS B&W PRINTERS	CLASS B&W PRINTER	UNCLASS COLOR PRINTERS	CLASS COLOR PRINTER	SHREDDERS	UPS	UNCLASS RACKS	CLASS RACKS
REGIONAL DISPATCH CENTER																																					
DISPATCH CELL																																					
OFFICE PERSONNEL																																					
RDC.DP.DM.01 (Dispatch Mgr Office)	1	1				1	1	1		1	1	2	1	1	1			1	1		2			1				1				1	1		2		
FLOOR PERSONNEL																																					
RDC.DP.DS.01 (Dispatch Mgr WS)	1	1				1	1			1		2		1	1			1				1													1		
RDC.DP.DS.02 (Dispatch Supervisor WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DS.03 (COMM Operator WS)	1	5				1	1			1		2		1	1			1				1													1		
RDC.DP.DO.01 (TECH Support WS)	1	5				1	1			1		2		1	1			1				1													1		
RDC.DP.DO.02 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.03 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.04 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.05 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.06 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.07 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.08 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.09 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.10 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.11 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.12 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.13 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.14 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.15 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
SUPPORT AREA																																					
DISPATCH LEADERSHIP SUPPORT ZONE							1																		1	1		1		1		1		1			
DISPATCH OPERATIONAL SUPPORT ZONE							1																		1	1		1	1	1		1		1			
DISPATCH CELL TOTAL	19	87	0	0	0	19	21	1	0	34	1	83	1	19	19	0	0	19	1	15	2	18	0	1	2	2	0	3	1	2	0	3	1	2	20	0	0

Minimum Acceptable Hardware Capacity Matrix

Table 19. Minimum Acceptable Hardware Capacity Matrix.

	SEAT	USERS	NMCI SEAT TYPE RED	NMCI SEAT TYPE WHITE	NMCI SEAT TYPE BLUE	NMCI SEAT TYPE S&T	UNCLASS LAN	CLASS LAN	OTHER LAN	UNCLASS PCs	CLASS PCs	MONITORS	KVM SWITCH	MICE	KEYBOARDS	LAPTOPS	LAPTOP FEEDS	UNCLASS PHONES	CLASS PHONES	OTHER PHONES	SPEAKERS	HEADSET	VTC	VIDEO DISPLAY	SCANNERS	UNCLASS FAX	CLASS FAX	WHITEBOARD	COPIERS	UNCLASS B&W PRINTERS	CLASS B&W PRINTER	UNCLASS COLOR PRINTERS	CLASS COLOR PRINTER	SHREDDERS	UPS	UNCLASS RACKS	CLASS RACKS
REGIONAL DISPATCH CENTER																																					
DISPATCH CELL																																					
OFFICE PERSONNEL																																					
RDC.DP.DM.01 (Dispatch Mgr Office)	1	1				1	1			1		2		1	1			1			1							1				1			2		
FLOOR PERSONNEL																																					
RDC.DP.DS.01 (Dispatch Mgr WS)	1	1				1	1			1		2		1	1			1				1													1		
RDC.DP.DS.02 (Dispatch Supervisor WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DS.03 (COMM Operator WS)	1	5				1	1			1		2		1	1			1				1													1		
RDC.DP.DO.01 (TECH Support WS)	1	5				1	1			1		2		1	1			1				1													1		
RDC.DP.DO.02 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.03 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.04 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.05 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.06 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.07 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.08 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.09 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.10 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.11 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.12 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.13 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.14 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
RDC.DP.DO.15 (Dispatch WS)	1	5				1	1			2		5		1	1			1		1		1													1		
SUPPORT AREA																																					
DISPATCH LEADERSHIP SUPPORT ZONE																																					
DISPATCH OPERATIONAL SUPPORT ZONE							1																		1	1		1	1	1		1		1			
DISPATCH CELL TOTAL	19	87	0	0	0	19	20	0	0	34	0	83	0	19	19	0	0	19	0	15	1	18	0	0	1	1	0	2	1	1	0	2	0	1	20	0	0

Communications Cell

The hardware capacities for the Communications personnel are given in the hardware matrices above.

Miscellaneous Rooms (Server Room and Video Teleconference Room)

Desired Capability and Assumptions

The desired capabilities for each personnel workstation within the miscellaneous rooms (Server Room and Video Teleconference [VTC] Room) are listed below. These desired capabilities are based on implemented system requirements and personnel requirements.

- In the VTC Room, personnel need the ability to view classified secret information and to easily modify the room into a Sensitive Compartmented Information Facility.
- The Server Room needs to hold 25 racks to support the implemented systems.
- A technician will be in the room to provide service support for the network and systems at the ROC/RDC.
- The VTC Room must be able to communicate with personnel located at remote locations.
- Personnel in the VTC Room need to view information generated on the ROC/RDC floor.

Desired Hardware Capacity Matrix

Table 20. Desired Hardware Capacity Matrix.

	SEAT	USERS	NMCI SEAT TYPE RED	NMCI SEAT TYPE WHITE	NMCI SEAT TYPE BLUE	NMCI SEAT TYPE SAT	UNCLASS LAN	CLASS LAN	OTHER LAN	UNCLASS PCs	CLASS PCs	MONITORS	KVM SWITCH	MICE	KEYBOARDS	LAPTOPS	LAPTOP FEEDS	UNCLASS PHONES	CLASS PHONES	OTHER PHONES	SPEAKERS	NON-USB HEADSET	VTC	VIDEO DISPLAY	SCANNERS	UNCLASS FAX	CLASS FAX	WHITEBOARD	COPIERS	UNCLASS B&W PRINTERS	CLASS B&W PRINTER	UNCLASS COLOR PRINTERS	CLASS COLOR PRINTER	SHREDDERS	UPS	UNCLASS RACKS	CLASS RACKS
MISCELLANEOUS																																					
OTHER ROOMS																																					
VTC ROOM	1	12				1	1	1		1	1	1	1	1	1		2	1	1				1	1				1							2		
SERVER ROOM 1	1	5				1	1	1		1	1	2	1	1	1			1	1		1							1							2	24	1

Minimal Acceptable Hardware Capacity Matrix

Table 21. Minimal Acceptable Hardware Capacity Matrix.

	SEAT	USERS	NMCI SEAT TYPE RED	NMCI SEAT TYPE WHITE	NMCI SEAT TYPE BLUE	NMCI SEAT TYPE S&T	UNCLASS LAN	CLASS LAN	OTHER LAN	UNCLASS PCs	CLASS PCs	MONITORS	KVM SWITCH	MICE	KEYBOARDS	LAPTOPS	LAPTOP FEEDS	UNCLASS PHONES	CLASS PHONES	OTHER PHONES	SPEAKERS	NON-USB HEADSET	VTC	VIDEO DISPLAY	SCANNERS	UNCLASS FAX	CLASS FAX	WHITEBOARD	COPIERS	UNCLASS B&W PRINTERS	CLASS B&W PRINTER	UNCLASS COLOR PRINTERS	CLASS COLOR PRINTER	SHREDDERS	UPS	UNCLASS RACKS	CLASS RACKS
MISCELLANEOUS																																					
OTHER ROOMS																																					
VTC ROOM	1	12				1	1	1		1	1	1	1	1	1			1	1				1	1				1							2		
SERVER ROOM 1	1	5				1	1	1		1	1	2	1	1	1			1	1		1							1							2	24	1

DETAILED DESIGN/EQUIPMENT LAYOUT

The critical front-end analyses that developed operational capabilities and derived system capacities now become the design requirements that allowed system designers and engineers (including HFEs) to develop candidate space and facility layouts for the ROC/ RDC. These designs now have a rationale and justifiable basis traceable all the way back to the NMETs.

At this stage in the design, the HFEs apply traditional human factors engineering/ergonomic scrutiny (i.e., MIL-STD-1472 design guidelines, ANSI, anthropometric data, etc.) to the physical design of the Operations Center. The following factors were considered in design development:

- Collaboration requirements
- Communication interfaces (internal/external)
- Traffic patterns
- Functional cell layout
- Visual display requirements (how many? location? how big?)
- Workstation design/ergonomics
- Audio requirements
- Lighting—general and task
- Seating—mobility, flexibility, comfort
- Ambient noise control

Figure 10 illustrates an initial design concept for the CNRSE ROC/RDC.

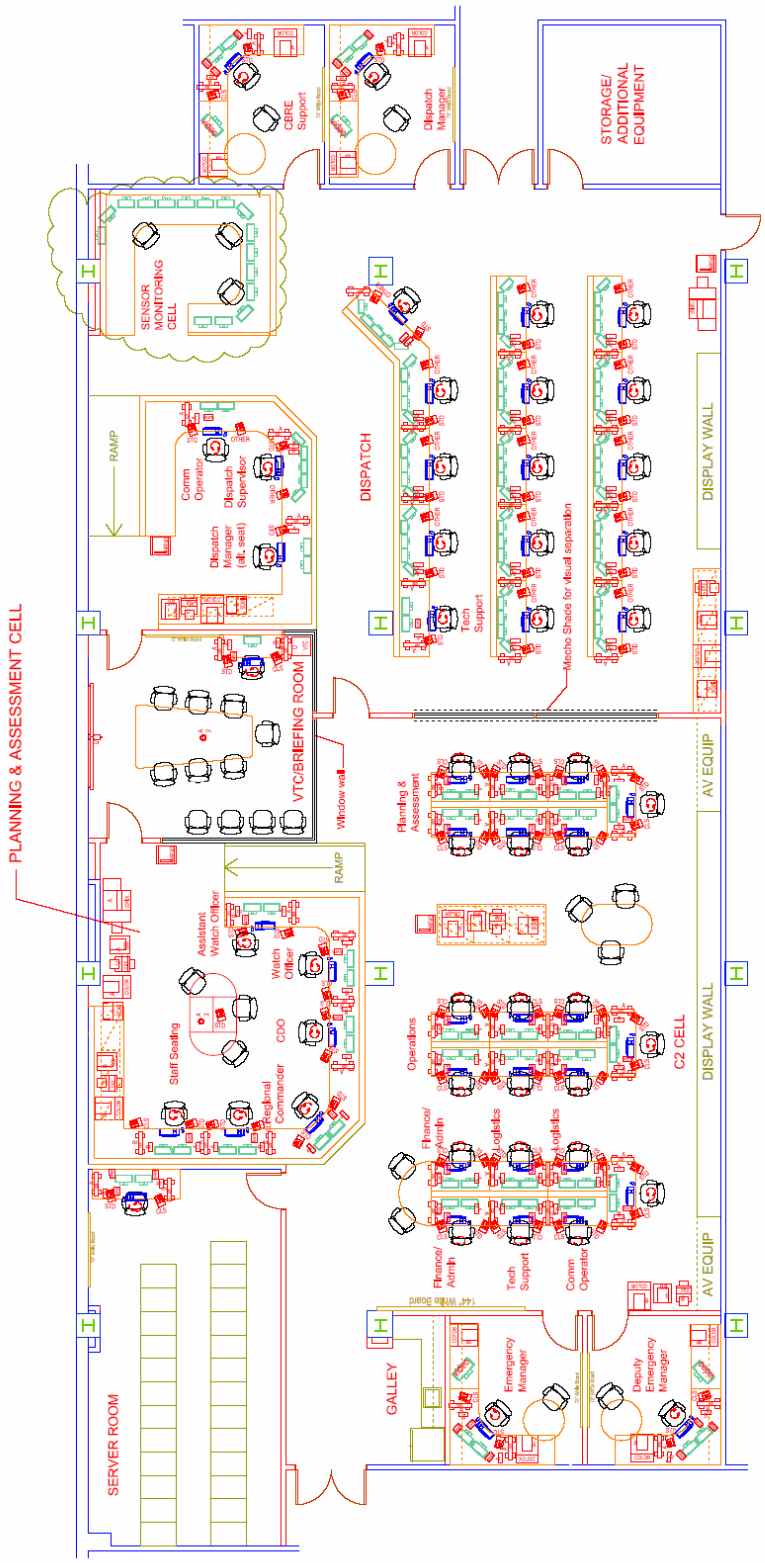

Figure 10. CNRSE ROC/RDC initial design concept.

CONCLUSIONS

The FUR methodology is a structured/repeatable process that allows systematic derivation of user requirements, providing traceability and justification of selected systems, tools, and applications. The process detailed in the preceding pages was used to drive the design, engineering, and architectural plans for the CNRSE ROC/RDC. The CNRSE ROC/RDC was completed and stood up for operations in May 2006. Commander Navy Installations Command and NAVFAC have deemed that it will be the template on which the remaining AT/FP ROCs and RDCs will be based.

RECOMMENDATIONS

SSC Charleston recommends the following Command Center Design improvements:

1. Require use of the FUR methodology for all AT/FP Operations Center programs (i.e., ROC, EOC, MCP)
2. Explore use of the FUR methodology in other AT/FP technology areas.

APPENDIX A

STATEMENT OF FRANK W. DEFFER

ASSISTANT INSPECTOR GENERAL, INFORMATION TECHNOLOGY

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING AND

TERRORISM RISK ASSESSMENT

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 13, 2006

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss the work of the Office of Inspector General (OIG) relating to DHS' system and approach for sharing counterterrorism, emergency management and intelligence-related information government-wide as well as the recommendations that we made to enhance departmental operations. My testimony today will address the evolution of the Homeland Security Information Network (HSIN); ongoing system planning and development activities; how well the system works to share information; and, major challenges to effective implementation. The information and recommendations that I will provide is contained in our report, *Homeland Security Information Network Could Support Information Sharing More Effectively* (OIG-06-38).

The Evolution of HSIN

State and local personnel have capabilities not possessed by federal agencies to gather information on suspicious activities and terrorist threats. By working together, government organizations can maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks. But earlier reports from congressional and industry organizations show that information on the threats, methods, and techniques of terrorists has not been shared routinely—and when information is shared it has not been consistently perceived as timely, accurate, or relevant.[1]

HSIN is a secure, unclassified, web-based communications system that provides connectivity between DHS' Homeland Security Operations Center (HSOC)—the national center for real-time threat monitoring, domestic incident management, and information sharing—and the critical private industry as well as the federal, state, and local organizations responsible for or involved in combating terrorism, responding to critical incidents, and managing special events. HSIN offers both real-time chat and instant messaging capability as well as a document library that contains reports from multiple federal, state, and local sources. The system supplies suspicious incident and pre-incident information, mapping and imagery tools, 24/7 situational awareness, and analysis of terrorist threats, tactics, and weapons. HSIN consists of a group of web portals organized along the lines of several community groups including law enforcement, emergency management, fire departments, homeland security, counterterrorism, and the National Guard. To fulfill its responsibility to coordinate the distribution of counterterrorism-related information across the various levels of government, DHS is expanding access to HSIN.

HSIN was created as an extension of the Joint Regional Information Exchange System (JRIES), begun in December 2002 as a grassroots pilot system to connect the California Anti-Terrorism Information Center, the New York Police Department, and the Defense Intelligence Agency (DIA) to facilitate the exchange of suspicious activity reports,

[1] *Efforts to Improve Information Sharing Need to Be Strengthened* (GAO-03-760, August 2003); *Protecting America's Freedom in the Information Age*, A Report of the Markle Foundation Task Force, October 7, 2002; *Creating a Trusted Network for Homeland Security*, The Second Report of the Markle Foundation Task Force, December 2, 2003.

register events potentially related to terrorist activity, and to foster real-time intelligence and law enforcement collaboration in a secure environment across federal, state, and local jurisdictions. JRIES proved useful during the northeast blackout in 2003 when information posted on the system allowed users across the country to quickly learn that the event was not related to terrorism. Although the DIA originally operated and maintained JRIES, DIA transferred program management of the system to DHS in September 2003, due to funding constraints.

After acquiring JRIES, DHS recognized that the system's utility could be expanded beyond its existing counterterrorism intelligence and threat awareness mission to support crisis planning, communications, and emergency management across federal, state, and local agencies. In 2004, the DHS Secretary renamed the system as HSIN in order to reflect its broader scope. DHS subsequently deployed HSIN to all 50 states, 53 major urban areas, five U.S. territories, the District of Columbia, and several international partners—extending HSIN access beyond the law enforcement community to include state homeland security advisors, governors' offices, emergency managers, first responders, the National Guard, and an international component. Because the system could not accommodate a large increase in users, DHS decided to migrate HSIN from the original software, Groove, to a series of web-based portals.2 DHS also launched an initiative to identify and address requirements of state and local communities of interest, as well as to provide robust training to promote effective use of the system. As of January 2006, eight states had adopted state-specific HSIN portals for use throughout their respective departments and agencies.

HSIN Planning and Development

Despite the vital role that HSIN was to play in ensuring intergovernmental connectivity and communications in a heightened counterterrorism environment, DHS did not follow a number of the steps essential to effective system planning and development. Specifically, DHS:

- rushed the HSIN schedule;
- did not clearly define relationships to existing systems;
- developed and deployed HSIN in an ad hoc manner;
- provided inadequate user guidance; and,
- did not establish performance metrics.

After assuming ownership of the system from DIA in 2003, DHS quickly expanded the system access to other user groups. Due to increased concerns and warnings about potential terrorist threats, the department's HSIN strategy was to implement a tool for nation-wide connectivity immediately and address operational problems and details later.

Such pressures to complete the system, however, created an environment that was not conducive to thorough system planning or implementation. For example, the rush to

[2] Groove Virtual Office is a Microsoft application that tracks contacts, alerts users to new activities, and provides a series of personal communications mechanisms.

implement resulted in inadequate definition of HSIN's role with respect to comparable law enforcement systems such as, Law Enforcement Online (LEO) and the Regional Information Sharing System Network (RISSNET); and, a failure to identify potential areas of duplication or opportunities for sharing information. Also, DHS developed the HSIN portals based solely on law enforcement requirements but did not sufficiently identify the needs of other HSIN user communities such as emergency management personnel and state homeland security advisors. Further, because DHS did not evaluate adequately the major HSIN releases prior to their implementation, technical problems that hindered system performance went undetected. Inadequate user guidance, training, and reference materials on what or how information should be shared resulted in some states defining information sharing processes and procedures on their own—activities that increased the potential for duplication of effort and lack of standardization. Additionally, DHS did not develop adequate performance measures. Instead it assessed HSIN performance based on tallies of active user accounts. Such numbers were neither a good indicator of system use nor the quantity of information shared using the system.

Some members of the law enforcement intelligence community raised concerns early on that DHS was expanding HSIN access and capability too quickly. For example, in an April 2004 issue paper, the executive board responsible for the predecessor JRIES stated that DHS was proceeding at a rapid rate in implementing the system and contended that this approach increased the risk of system misuse, security breaches, privacy violations, and user confusion as well as dissatisfaction. The board pointed out that the department's newness and its lack of established relationships hampered its ability to quickly gain the trust and commitment of states and major cities to the HSIN approach.

HSIN Information Sharing Effectiveness

We found that, largely due to the planning and implementation issues discussed, users are not fully committed to the HSIN approach. Specifically, state and local users we interviewed provided mixed feedback regarding HSIN. Although they generally like the web portal technology, they have several suggestions on how to improve the system's technical capabilities to meet their needs. Users do not fully understand HSIN's role and how the information shared on the system is used, either. Last, situational awareness information that could help states and cities determine how to respond to threats when major incidents occur is not readily available. The HSIN-Secret portal, meant to function as a temporary channel to deliver classified information, does not provide valuable terrorism-related content.

Some users in the law enforcement community told us that they do not trust the system to share sensitive case information. This erosion in trust as the system was expanded led to conflicts between the JRIES executive board, comprised primarily of law enforcement officials, and HSIN program management. In May 2005, concerned with the direction that DHS had taken with JRIES/HSIN without soliciting its input, the JRIES executive board voted to discontinue its relationship with the HSOC. The consensus of the board was that the HSOC had federalized what it believed to be a successful, cooperative federal, state, and local project. After their withdrawal, the JRIES executive board continued to promote its initial information-sharing concept as JRIES II, a separate system apart from HSIN, which has confused state law enforcement personnel.

Because HSIN does not fully meet their needs, users do not rely upon the system to share counterterrorism information. For example, law enforcement users said that they often use other existing systems, such as Law Enforcement Online, the Regional Information Sharing System Network, and the Federal Protective Services-Secure Portal System. Private systems, such as the "NC4" managed by the National Center for Crisis and Continuity Coordination, provide real-time information to state and local subscribers. The system provides warnings, alerts, and situational awareness on a fee for service basis. In some instances, agencies such as the U.S. Secret Service are creating their own portals for information sharing among a limited user group. Such practices perpetuate the ad hoc, stove-pipe information-sharing environment that HSIN was intended to correct.

Further, state and local law enforcement officials said that they continue to depend upon personal contacts and telephone calls to related organizations to exchange intelligence on potential threats. These users recognize, however, that phone calls are not the most efficient means of obtaining situational awareness information and coordinating incident response activities. For example, users stated that during the 2005 London bombings, they needed timely information, such as whether the attacks were suicide attacks, so that state and local transportation security would know what to look for in their own jurisdictions. However, the information provided on HSIN was no more useful or timely than information available via public news sources. Users were able to get better information faster by calling personal contacts at law enforcement agencies with connections to the London police, than by using the system.

Along with a continued reliance on alternative means to share information, state and local users are making limited use of HSIN. Although law enforcement is a principal HSIN customer, officials at state fusion centers and police counterterrorism units said that they do not use the system regularly to share intelligence information.[3] Officials at nine of the 11 state and city emergency operation centers that we visited stated that they log on to the system only occasionally. Further, some emergency operation centers have a very limited number of user accounts, while others are not connected to HSIN at all.

Data provided by HSIN program management demonstrates that user logons and postings are limited, and that users do not view the system as the nation's primary information sharing and collaboration network as DHS intended. Although the total number of HSIN user accounts has increased since the system was deployed, use of three of the primary HSIN portals—the law enforcement, emergency management, and counterterrorism portals—has remained consistently low.

[3] Fusion centers are two or more agencies collaborating to provide resources, expertise, and/or information to maximize the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.

Major Challenges

In addition to the technical system issues discussed above, DHS faces multiple challenges, often beyond the control of HSIN program management to successfully implementing HSIN to support homeland security information sharing. First, resource limitations have hindered the ability of organizations at all levels of government to effectively share information. This will undoubtedly continue to pose challenges in the future. For example, DHS officials cited a lack of sufficient personnel as a reason for their inability to provide vital support to HSIN users, especially during its initial release. Similarly, state officials expressed concern that they do not have enough personnel to monitor all of the federal systems available to them. For example, a state emergency management official said that, at one point, a single employee had to monitor 19 different systems. State officials added that a lack of funding limits their ability to sustain operations at state-run facilities, such as intelligence fusion and analysis centers, too.

Second, legislative requirements have created challenges to effective information sharing. Federal legislation over the past several years has established new goals and authorities for information sharing beyond those initially assigned to DHS. The *Homeland Security Act of 2002* gave DHS the responsibility to coordinate and share information related to threats of domestic terrorism with other federal agencies, state and local governments and private sector entities. In 2004, however, the *Intelligence Reform and Terrorism Prevention Act* established the Office of the Director of National Intelligence external to DHS. The act mandated the establishment of an information-sharing environment under the direction of a newly designated program manager to facilitate sharing of terrorism-related data nation-wide. Establishing this new information-sharing environment will involve developing policies, procedures, and technologies to link the resources of federal, state, local, and private sector entities to facilitate communication and collaboration.

State laws, which differ widely, also may conflict with federal collaboration initiatives and, in some cases, prevent effective information sharing. For example, DHS has little authority to require that state and local governments or other user communities use HSIN for information sharing. As such, department officials often find themselves in a consultation mode with the states. Alternatively, state laws, which may be very restrictive, can limit the ability of state and local user communities to share information through HSIN. Law enforcement communities, for example, are governed by laws that prohibit sharing certain types of sensitive information.

Third, privacy considerations cannot be ignored in the context of information sharing. Specifically, maintaining the appropriate balance between the need to share information and the need to respect the privacy and other legal rights of U.S. citizens can be a difficult and time-consuming effort. Due to privacy concerns, civil liberties organizations have challenged information-sharing initiatives in the past and could pose similar challenges for the HSIN program.

In 2003, the American Civil Liberties Union raised concerns about the Multistate Anti-Terrorism Information Exchange (MATRIX) system, an effort to link government and commercial databases to enable federal and state law enforcement to analyze information as a means of identifying potential patterns of suspicious activity by individuals. As a result of the privacy concerns raised, as well as the costs involved, many state law enforcement communities stopped using the Multistate Anti-Terrorism Information Exchange system.

Failure to consider privacy concerns could result in similar abandonment of HSIN before its full potential is realized. As required by the *Homeland Security Act*, and in an effort to assuage civil liberty concerns, DHS performed a privacy impact assessment of HSIN portals before deploying them. As a result, DHS had to shut down the HSIN document library which contained reports from nation-wide sources, significantly hampering system usefulness. In addition, DHS is creating another database subject to a privacy impact assessment prior to its implementation. This database will provide intelligence analysis capability similar to that of the abandoned Multistate Anti-Terrorism Information Exchange system. Besides the privacy impact assessment, clear standards and effective controls will be needed to demonstrate to concerned consumer groups that the information gathered through HSIN does not violate the rights of American citizens.

Fourth, a culture that is not receptive to knowledge sharing is one of the foremost hurdles to widespread adoption of the HSIN collaboration software. HSIN users comprise diverse communities, including state and local government officials, emergency managers, law enforcers, intelligence analysts, and other emergency responders. Each has different missions, needs, processes, and cultures. Because of these differences, often the various user groups are reluctant to share information beyond the bounds of their respective communities. Traditionally, for example, law enforcement has operated in a culture where protecting information is of paramount concern. Shifting from this “need to know” culture to a “need to share” culture has proven difficult. DHS officials anticipated when they first released HSIN that culture might become an issue, but they did not have the time or resources to build the trusted relationships necessary to overcome this issue.

Identifying and understanding such user community goals and requirements are a first step to understanding cultural differences and building collaborative relationships. Frequent communication, guidance on how shared information will be used and protected, effective feedback, and mechanisms for resolving issues in a timely manner can also serve to overcome differences and instill trust and understanding.

Conclusions and Recommendations

DHS has a critical role to play in ensuring national awareness, preparedness, and coordinated response to potential emergency situations, suspicious activities, and terrorist threats. HSIN can assist by supporting timely and relevant information exchange among the federal, state, local, and private organizations that need to share counterterrorismrelated data to carry out their respective missions. However, the many system planning

and implementation issues, as well as other related challenges, that I have outlined have hindered DHS' ability to fulfill its central coordination role and to provide the communications and IT infrastructure needed to keep our homeland secure.
To ensure the effectiveness of the HSIN system and information sharing approach, we recommended in our report that the Director, Office of Operations Coordination, Department of Homeland Security:

1. Clarify and communicate HSIN's mission and vision to users, its relation to other systems, and its integration with related federal systems.
2. Define the intelligence data flow model for HSIN and provide clear guidance to system users on what information is needed, what DHS does with the information, and what information DHS will provide.
3. Provide detailed, stakeholder-specific standard operating procedures, user manuals, and training based on the business processes needed to support homeland security information sharing.
4. Ensure cross-cutting representation and participation among the various stakeholder communities in determining business and system requirements; and, encourage community of interest advisory board and working group participation.
5. Identify baseline and performance metrics for HSIN, and begin to measure effectiveness of information sharing using the performance data compiled.

The Acting Director, Office of Operations Coordination, concurred with our recommendations in their entirety. Further, the Acting Director noted that the recommendations are solid, and when implemented, will improve the HSIN system and information sharing effectiveness.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention and welcome any questions from you or Members of the Subcommittee.

APPENDIX B
SITE VISIT HSI OBSERVATIONS

HSI ISSUE	SITE
Physical Security	
No local security surveillance	OT-28
Building security marginal	OT-28
Building too close to street	OT-28
Room not secure	OT-28
Physical	
No direct line between OT-28 and SCC-J	OT-28
Video wall poor placement	OT-28
Poor layout / Changes as systems are dumped	OT-28
Video wall views limited and obstructed	OT-28
Fire sprinkler systems located above video wall	OT-28
Screen burn-in on displays	OT-28
No panorama video views	OT-28
Uncomfortable chairs	OT-28
Poor communications setup for node-to-node	OT-28
Process	
Workload when multiple incidents	OT-28
Workload - moving from Metro to Region AOR	OT-28
No training scenarios	OT-28
No systems support?	OT-28
Have to deal with a number of paper documents (tables)	OT-28
Only do limited number of drills	OT-28
Long shifts	OT-28
No SOPs	OT-28
No pre-planned responses	OT-28
No written SOP for boat house	OT-28
Informal pass-down	OT-28
No checklists	OT-28
Inter-agency conflicts of info	C3F
30% - 40% of the time spent reviewing message traffic	C3F
<u>DO NOT</u> miss the important message	C3F

System / Software	
Watchstander usually reboots system (Vistascape?) in the morning	OT-28
Don't have latest version of Vistascape	OT-28
Wind/speed/direction for Chem-Bio event	OT-28
SIPRNet not available because of security considerations	OT-28
Small unviewable font in one display	OT-28
Could use directional info on camera displays	OT-28
Like to have panoramic view of Vistascape	OT-28
No common tactical picture between EHSS and SM10	OT-28
No blue force tracking (patrol boats)	OT-28
Messages manually entered into status board	OT-28
Unused systems	OT-28
Workstation not setup for 24/7	OT-28
Multiple "locations" within space hold data needed to complete tasks	C3F
Training / Manning	
No systems training	OT-28
W/C being pulled from law enforcement into force protection	OT-28
Not all dispatchers are cleared	OT-28
No formal job descriptions	OT-28
Undefined job descriptions	OT-28
Lack of training on systems	OT-28
Not trained in Intel analysis (JPEN/ASOCC)	OT-28
Personnel selection not AT/FP qualifications based	OT-28
Undermanned for requirement of monitoring 80+ cameras	OT-28
OT-28 watchstander not a billeted position	OT-28
People working outside of job descriptions	OT-28
Junior/low skill personnel	OT-28
Watch commander not AT/FP trained	OT-28
Fleet Watch Officer is the only full-time billet	C3F
Message traffic sorting rules (guidance) - training implications	C3F
"Need a proactive team that understands nuances"	C3F
Detect. Assess. Respond.	OT-28
User guide is a Capivate tutorial	OT-28

APPENDIX C

RDC SITE VISIT REPORTS

RDC Ethnographic Study-Field Observations

RDC Site Visit #1 Conducted on 21 February, 2005

RDC Site Visit #2 Conducted on 26 October, 2005

RDC Site Visit #1 Report

Date: 21 Feb 2005

To: KE Team

From: Human Factors Engineer

Subject: Task- and User-Centered Observations from Site Visits in Support of the IMPP Project

The following observations were made from a task- or user-centered perspective in an effort to gain insight into the role of the command center, watchstation, and/or watchstander. This information will be used to facilitate future interviews, identify potential usability research & analysis areas, and ultimately help determine how the IMPP software may be designed to meet the needs of the user. This is a first-pass assessment of the various sites and is in no way intended to be a complete site analysis.

The observations are categorized by, 1) the site visited, then 2) a related-observation grouping (i.e., all site observations regarding watchstations are grouped under a category heading titled, "watchstations", etc.).

The sites visited during the period of 16-17 February 2005 are as follows:

- US Coast Guard Sector Command Center (SCC)
- US Coast Guard Joint Rescue Coordination Center (JRCC)
- Regional Dispatch Center (RDC)
- Commander Naval Region X Regional Command Center (RC).

Regional Operations Command (RDC) Region X Harbor site visit conducted on Thursday, 17 Feb 2005

Center Chief conducted the site visit.

Responsibilities: The RDC is responsible for dispatching all fire and emergency medical service (EMS) calls for all military bases on Region X. The ROC is also responsible for security issues on the Navy bases; the Army and Marine Corp handle their own security issues on their facilities. (note: although the Army & Marine Corp handle their own dispatching for security issues, they are still operating from the RDC server system.)

Workload: The RDC personnel handle a call load of 286,000 events per year.

Watchstations/Dispatchers

- 911 Dispatcher (two personnel)
- Waterside Security (the POC)
- Shipyard Security Watch
- Fire Calls – (handles fire calls for all bases)
- Region X Harbor Security
- Naval Magazine Security
- Army Security (not currently manned)
- Marine Security (not currently manned)
- Dispatch Center for NC IO
- Watch Supervisor

Manning Issues

- The RDC currently has a staff of 29 people, but based on a manning assessment performed by Emergency Services Consulting, Inc. (ESCI) they should have 37 staff members.
- All stations are interchangeable. When the user signs in as a specific role the Computer Aided Dispatch (CAD) knows to forward all calls that fall under that role's area of responsibility.
- All dispatch operators are interchangeable because they all receive training in the different roles (e.g., First Responder, EMS dispatch, telecommunications, CPR, etc.). All dispatchers are currently government workers (now a GS 6/7 position).
- It appears that the ORBACOM system can handle the work that is currently being performed by the watchstanders in the RC (see task description in the RC section below). Personnel within the RDC had also suggested this.

Automation Issues

- To make up for their shortage of personnel the RDC is making use of automation (currently or intending to in the future?). For example, they have (now?) the fire and intrusion alarms passing straight through the RDC and directly to the responsible unit.
- The "Resource – RDC" display (by ORBACOM Systems, Inc.) acts as an automated phone tree. Calls can be auto-forwarded to the responsible parties and if that parties' line is busy then the system will go down the list and try the next number.

Workload Management: The CAD will send incoming calls to a dispatcher not currently involved with a call. It appeared that the CAD also implements some type of workload manager and alternated sending incoming calls to from one dispatcher to the next in an attempt to spread the workload across all dispatchers. Dispatchers have the ability to pick up a call even though it was send to a different dispatcher.

Usability Issue: Sentinel 911 system – handles 911 calls from base housing. There is currently an issue with the telecommunication provider wherein CAD cannot receive a location from calls originating within base housing. Calls from base housing are automatically forwarded to the Sentinel 911 system, which has the ability to obtain an exact location within base housing. If there is a real emergency, the dispatcher will start an incident report in the CAD and manually transfer the information from Sentinel 911 to the CAD.

Information Displays

There are currently 9 large front projection screens in the RDC. The information displayed on the screens is as follows:

1. Shipyard gate camera (this screen is located at back of the RDC)
2. NAVMAG gate camera (this screen is located at the back of the RDC)
3. Waterside security cameras
4. Map of Fire calls (controlled by Fire Calls dispatcher)
5. Region X Harbor security cameras (fed from the RC)
6. CNN and other television signals
7. NAVMAG nighttime motion activated cameras
8. Other feed from RC (?)
9. Not used – reserved for possible use by Army or Marines

They are slated to get a video feed from Navy Command X to monitor six access doors to the Navy Command X building.

Miscellaneous Information

- The RDC would like to merge their CAD with the Region X Fire & Police departments.
- Contractor 1 did the phase I design and layout of the RDC. Contractor 2 is tasked to do phase IV upgrades and room expansion to the RDC in FY06.
- They have funding in place to connect the RDC to the RC, should be complete by Summer 2005. (Not sure what information they are going to pass with this new connection.)
- NMCI is only used for e-mail. Their applications are not NMCI approved so they must use the two different systems.
- A CONOPS has already been created for the RDC; Emergency Services Consulting, Inc. (ESCI) created it during their manning analysis.
- "Nothing in the world of emergency response is classified data. It runs on a secure net, but the data is not classified."

RDC Field Trip #2 Report

Date: 26 October 2005

To: KE Team

From: Human Factors Engineer

Subject: Task- and User-Centered Observations From Regional Dispatch Center (RDC) Site Visit Conducted on 26 October 2005 in Support of the IMPP Project

---

The following observations were made from a task- or user-centered perspective in an effort to gain insight into the tasks being performed by the dispatchers and/or watchstanders in the dispatch center.

Regional Dispatch Center X (RDC X) Site visit conducted on Wednesday, 26 October 2005

Miscellaneous Items

- Region X's RDC is under the Federal Fire Department, Region Y's RDC is under Federal Police.
- Future capability – they plan to replace the Navy pier sentries with a camera & automated gate. The sailor requesting access to the pier will hold a photo ID up to a camera, that image will be placed on a large screen display for the dispatcher to review. If appropriate, the dispatcher will unlock the gate via a remote gate control.
- They are either planning, or have already completed, installing a Computer Aided Dispatch (CAD) terminal and watchstander in the Regional Operations Center (RDC)
- Region X Harbor does not use Dunlop barriers like Region Y harbor.
- Would like to relocate the RDC to a more secure facility.
- They track the location of Region X Harbor security forces (through the use of?).

Manning Issues

- Their dispatchers/watchstanders run three 8-hour shifts.
- Currently staff three 911 dispatchers and two Federal Fire dispatchers (can double as 911 dispatchers in heavy load situations)
- Currently have a Shipyard Security watchstander/dispatcher. He monitors for shipyard alarms.
- Region X Detachment provided a system administrator to Center Chief.
- Center Chief is trying to convert his two shipyard watchstanders to contract employees…avoid pulling the employees in different directions at different times.
- Dispatcher on duty:
    - ♦ Day watch = 7 dispatchers
    - ♦ Swing shift = 6 dispatchers
    - ♦ Mid shift = 5 dispatchers
- Have 11 contractors on-site with room for 2 more.
- When hiring, they really look for a young, inexperienced but computer savvy person that is a fast typist.
- Hiring good personnel is a real issue…usually must try to hire contractors to get around the "good quality" people issues.
- RDC would like to make the EHSS operator a civilian position so he can rotate that watchstander through the other dispatch positions (cross-training).

- RDC staff:
    - ♦ 21 Government GS employees (includes Center Chief & 2 other supervisors)
    - ♦ 11 Contractors

Automation Issues

- They receive their "Tug Report" electronically via the RSIMS. This report is generated by Facilities personnel not co-located in the RDC.

Workload Issues

- They rank their most important dispatching to be Emergency Medical Services (EMS).
- The RDC handles all 911 calls for all bases in Region except for Region X Air Force Base.
- The RDC dispatches Fire for all bases (Army, Navy, Marines, Air Force?)
- The RDC dispatches Security for only Navy bases.
- Looking into adding Security dispatch for Camp XYZ and Marine Base.
- The CAD software has (or can be added) a workload management component which helps answer questions related to human resources, manning, identify who is/isn't handling their share of the workload and determining which are the busiest positions.

Communication Issues

- The RDC now has a radio link to the Coast Guard facility.
- Would like to share their dispatch information with the Region X Fire Department & Region X Police Department.

Information Displays

- When entering information into CAD, the location of the incident is displayed on the large LCD monitor mounted over their workstation. (Not sure if this location is based on the telephone company's 911 address or something entered by the dispatcher.)

Information Systems

- Their CAD system will be replaced by NERMS (Navy Emergency Management System). (note: Northrop Grumman won the contract to build NERMS, Hawaii's RDC was already using the Northrop Grumman system so their transition impact should be minimal.)
- "Enhanced 911" is for on-base housing locator (give address of origin for 911 call initiated from on-base housing).
- MAS (MasterMind Monitoring) system handles incoming alarms. It presents all information regarding an alarm/sensor. The MAS can send the alarm information to the CAD for further tracking and dispatching. (not sure if the contractor made the software link between MAS and the CAD) When in CAD, the alarm will auto-fill with most of the alarm information…dispatcher may still have to enter some information not brought into CAD from MAS.
- The RDC has remote CAD sites located at the Marine base and at Region X Barracks. The system is called "VelociCAD".
- NERMS will include CAD, RMS (records management system) and MDC (mobile data computers). NOTE: It will not have a vehicle locator system.
- Navy Magazine (NAVMAG) security is provided by the use of cameras and sensors (alarm monitoring).
- They have an automated radio communications recorder.
- They have a workflow system that forwards information to an available dispatcher. (not sure what the trigger is for this workflow…911 call or alarm)

- Triage Checklist by ProKey. Allows dispatcher to walk through a series of questions & actions to handle an incident.
    - ♦ Shipyard incidents (spillages, etc.) answers questions and guides the dispatcher to the next questions to ask.
    - ♦ Provides auto-notification to the proper personnel when you reach a certain point in the sequence.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-01-0188*

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
10–2006	Final	

4. TITLE AND SUBTITLE

USING HUMAN SYSTEMS INTEGRATION AND KNOWLEDGE ENGINEERING TO DEFINE AND DESIGN ANTI-TERRORISM/ FORCE PROTECTION SYSTEMS AND SOLUTIONS

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHORS

D. Lulue
G. Wilford
D. Gill-Hesselgrave

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

SSC San Diego
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

TR 1949

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Naval Facilities Engineering Command
1322 Patterson Avenue, S. E. Suite 1000
Washington Navy Yard
Washington, DC 20374-5065

10. SPONSOR/MONITOR'S ACRONYM(S)

NAVFAC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

This is the work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction. Many SSC San Diego public release documents are available in electronic format at http://www.spawar.navy.mil/sti/publications/pubs/index.html.

14. ABSTRACT

This report provides study analyses, findings, and improvement recommendations based on work domain data collected by SSC San Diego and SSC Charleston. "Worked examples" of how to best use Human Systems Integration (HIS), Knowledge Engineering (KE), Business Process Modeling (BPM), and User-Centered Design (UCD) elements to investigate, model, and re-engineer AT/FP processes are included. The authors' hypothesis throughout their investigations was that by following these processes and applying the principles of HSI, KE, BPM, and UCD, key decision-makers and customers of the acquisition process can make more informed decisions. The report also includes conclusions and recommendations from the SSC San Diego and SSC Charleston team studies.

15. SUBJECT TERMS

Mission Area: Human Factors Engineering

human systems integration	knowledge engineering	process modeling
command and control	user-centered design	functional user requirements

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			D. Gill-Hesselgrave
U	U	U	UU	69	**19B. TELEPHONE NUMBER** *(Include area code)* (619) 553–6679

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

INITIAL DISTRIBUTION

20012	Patent Counsel	(1)
21511	J. Andrews	(1)
21512	Library	(2)
21513	Archive/Stock	(3)
24610	D. Gill-Hesselgrave	(10)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (1)

SSC San Diego Liaison Office
C/O PEO-SCS
Arlington, VA 22202–4804 (1)

Center for Naval Analyses
Alexandria, VA 22311–1850 (1)

Government-Industry Data Exchange
Program Operations Center
Corona, CA 91718–8000 (1)